(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 966 145 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.12.1999 Bulletin 1999/51

(51) Int Cl.6: H04M 7/00, H04L 12/66

(21) Application number: 99870128.8

(22) Date of filing: 21.06.1999

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 19.06.1998 US 90038 P

(71) Applicant: Nortel Networks Corporation
Montreal, Quebec H2Y 3Y4 (CA)

(72) Inventors:
- Brivet, Mayeul
94350 Villiers sur Marne (FR)
- Tripps, John
75004 Paris (FR)
- Aubry, Isabelle c/o Nortel Europe S.A.
Bussy-St-Georges, 77608 Marne-la-Vallée (FR)

(74) Representative: Bird, William Edward et al
Bird Goen & Co.,
Termerestraat 1
3020 Winksele (BE)

(54) IP telephony gateway

(57) The present invention provides an IP telephony gateway. According to a first aspect of the invention, the gateway provides communications between a switched circuit network (SCN) and an IP network. The gateway can handle calls between clients on the switched circuit network and IP clients on the IP network. The gateway provides supplementary call services/features for calls to/from IP clients on the IP network, thus providing IP clients with similar features to those that are available to terminals on a PBX. The gateway is preferably a PBX which supports the supplementary services/features.

Advantageously, the gateway can also provide supplementary call services/features to calls between IP clients on the IP network. This can be achieved by routing call control signaling for IP client - IP client calls via the gateway where the services can be controlled.

A further aspect of the invention provides an IP network in which IP clients have access to a range of supplementary call features/services. At least one of the supplementary features/services is provided by a gateway, such as a PBX, at an interface to the IP network. A call from an IP client is routed via the gateway to apply the supplementary feature/service.

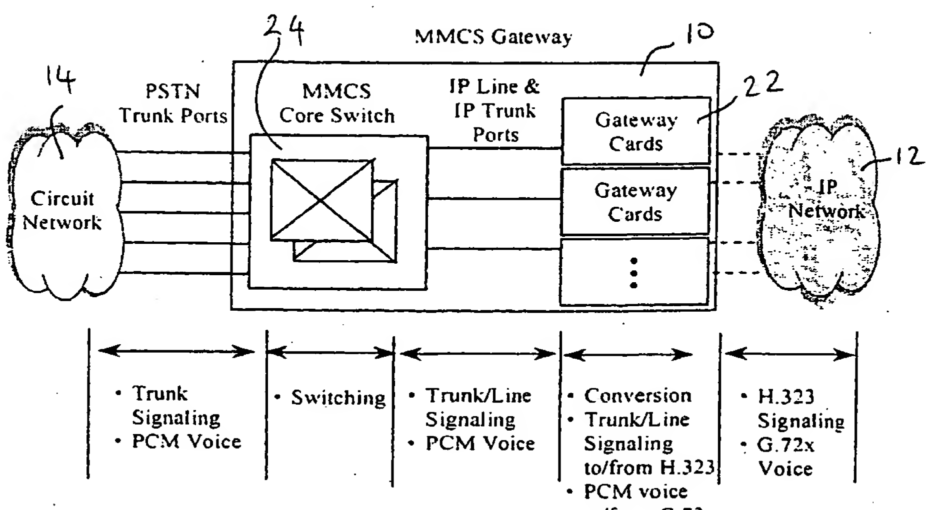


Fig. 3

EP 0 966 145 A2

Description

[0001] The present invention relates to an IP line side IP telephony gateway and a network using the same as well as to methods of operating the gateway and the network, in particular to methods and apparatus for providing supplementary services to IP telephony networks.

TECHNICAL BACKGROUND

[0002] Data networks operators, cable TV operators and other carriers want to offer customers good voice quality and telephony services over their IP networks. To achieve this goal, it is required to provide IP terminals (either client software running on PCs or specialized "IP phones") having the same level of functionality that is available to sets connected to a PBX. As carriers build new voice networks based on IP Telephony, they need a bridge to the legacy circuit switched networks. IP Telephony gateways provide this bridge between traditional circuit switched networks and emerging voice services based on IP networks and technology. A Line-side Gateway enables a circuit switched central office switch to provide line-side services to terminals deployed on IP data networks (i.e. IP-based replacement ofthe subscriber loop access). A Trunk-side Gateway enables a circuit switched central office switch to route inter-switch traffic via IP data networks, bypassing circuit switched trunk facilities.

[0003] Various terms such as "Internet Telephony", "Voice Over IP" (VoIP), and "Voice and Fax over IP" (XoIP) are used in the IP Telephony industry to describe IP network based telephony services. With respect to this invention, the term "IP Telephony" is used to describe voice and fax services transported over managed IP networks engineered for quality IP Telephony services as opposed to "Internet Telephony" which refers to voice & data transported over the unmanaged Internet.

[0004] The Internet is a collection of independent networks with high capacity in only some of the participating networks, limited security, service disruptions, and no standardized means to guarantee the Quality of Service (QoS) between the networks, or even within a network. Of these issues, the inability to guarantee a QoS across the networks is the main issue impacting telephony services such as voice which requires low latency in IP packet transmissions and fax which requires that all packets be delivered without losing information. As such, the Internet currently provides a poor platform for telephony services.

[0005] Managed IP networks, on the other hand, which typically have high capacity and can manage QoS criteria such as end to end latency and packet loss, provide a better platform for IP Telephony services. Hence, IP Telephony services will only be deployed successfully in the near term on managed IP networks.

[0006] IP Telephony began in about 1995 with PC hobbyist's using proprietary solutions to bypass the Public Switched Telephony Network (PSTN) by making PC to PC calls free through the Internet. The calling party typically accesses network database to identify PCs which are on-line and available to call. The calls are characterized by unpredictable voice quality and high latency due to the dependency on the Internet as the transport network. In order to capitalize on the difference in tariff structures between the PSTN and the Internet, IP Telephony Service Providers have launched IP Telephony services that can be used by the general public as well as businesses to make and receive long distance calls from standard phones and fax machines at significantly reduced rates. The calling party uses a multi-stage dialing plan to dial a local or toll free number to access the IP Telephony Service Provider's network, enter a billing ID such as a calling card or authorization code, and then dial the destination to be called. With Fax machines, an autodialer at the calling party's premises must be used with the IP Telephony service in order for it to be transparent to the Fax machine. As well, IP Telephony Gateway's must be positioned between circuited switched network and the IP network as a bridge between the packet switched IP network and the circuit switched world. As the user interface and voice quality of PC-based IP Telephony solutions continues to improve, the volume of IP Telephony calls originating on a device in the IP network and terminating to a device in the circuit switched network (and visa versa) will continue to increase. The device in the circuit switched network is typically a standard phone or fax machine. A PC running IP Telephony Client software is currently used as the device in the IP network. However, vendors are beginning to introduce IP Telephony terminals which give the user the option of using a standard phone interface to an IP Telephony service. An example of such as terminal is the M9617 USB phone recently introduced by Nortel Networks, Canada. An IP Telephony Gateway is required as a bridge between the IP network and the circuit switched network.

[0007] It is an object of the present invention to provide an IP line side IP telephony gateway and a network using the same as well as to methods of operating the gateway and the network which do not suffer from the problems of the prior art.

[0008] It is a further object of the present invention to provide an IP line side IP telephony gateway and a network using the same as well as to methods of operating the gateway and the network which allow optimum use of resources of the IP telephony gateway.

[0009] It is still a further object of the present invention to provide an IP line side IP telephony gateway and a network using the same as well as to methods of operating the gateway and the network provide an economical integration of

components.

[0010] It is yet a further object of the present invention to provide an IP line side IP telephony gateway and a network using the same as well as to methods of operating the gateway and the network in particular to methods and apparatus for providing supplementary services to IP telephony networks.

SUMMARY OF THE INVENTION

Supplementary services/features

[0011] According to a first aspect of the invention, a gateway provides communications between a switched circuit network (SCN) and an IP network. The gateway can handle calls between clients on the switched circuit network and IP clients on the IP network. The gateway provides supplementary call services/features for calls to/from IP clients on the IP network, thus providing IP clients with similar features to those that are available to terminals on a PBX. The gateway is preferably a PBX which supports the supplementary services/features.

[0012] Advantageously, the gateway can also provide supplementary call services/features to calls between IP clients on the IP network. This can be achieved by routing call control signaling for IP client - IP client calls via the gateway where the services can be controlled.

[0013] A further aspect of the invention provides an IP network in which IP clients have access to a range of supplementary call features/services. At least one of the supplementary features/services is provided by a gateway, such as a PBX, at an interface to the IP network. A call from an IP client is routed via the gateway to apply the supplementary feature/service.

[0014] A switch/PBX is connected to an IP network and provides at least one supplementary call feature/service to an IP client in the IP network.

[0015] The features/services can be one or more of the following:

- originating restrictions;
- terminating restrictions;
- call forwarding (CFB, CFNA, CFU, CFNR);
- calling line identification (CLID);
- CLID restriction;
- calling name display;
- call transfer.

While call signaling for IP client - IP client calls is routed via the gateway, voice traffic is preferably routed directly between the IP terminals without passing via the gateway. When voice traffic for IP client - IP client calls is routed via the gateway, the gateway can arrange to route the voice traffic directly between an input and an output of the gateway without the need for a double decode/encode of the voice traffic thereby avoiding voice quality degradation. Advantageously some supplementary services can be provided by another part of the IP network. Advantageously, supplementary services can be provided by a gatekeeper. This can be achieved by signaling between the gateway and the gatekeeper or directly between the IP client and the gatekeeper. Advantageously, services can be provided by an application connected to the IP network, with signaling between the gateway and application via the IP network to apply the service.

Gateway ports

[0016] According to a further aspect of the invention a connection between a gateway and an IP client in an IP network is provided by an IP line from the gateway. The gateway has a pool of IP line ports which can be used for the connections to the IP clients. The IP line ports are a shared resource which are assigned to a client for the duration of an IP call and then released back to the pool of IP line ports to be used by another client. Thus an IP line port is assigned to an IP line on a call-by-call basis. This reduces the number of ports that are required to serve a given number of IP clients in the IP network.

[0017] Preferably, while an IP line port is assigned to a client, the IP line port assumes the attributes of the client's line data. Thus subscriber services such as call forwarding, calling line ID and specialized dialing plans can be processed for that client while that client's line data is associated with the IP line port.

[0018] An IP client can be identified by a virtual directory number (VDN) and an available port by a physical terminal number.

[0019] The core switch can store information about the state of IP clients that it is serving, such as whether they are busy. Thus, upon receiving an incoming call from the switched circuit network, which is directed to a busy IP client, the

switch can provide an appropriate treatment and reduce signaling within the system.

Address resolution

[0020] According to a further aspect of the invention, conversion between address formats for calls to IP clients is performed at a gateway to an IP network. The conversion is between the LAN alias or directory number (DN) of a terminal and an IP address. According to one embodiment, an address table is downloaded from a gatekeeper for use at the gateway. According to a second embodiment the gateway stores a list of most recently used and/or most recently called addresses. In both embodiments, if an address cannot be converted using the information stored at the gateway, a request is made to the gatekeeper. In a preferred embodiment a gatekeeper handles all address resolution and a DN table is uploaded from the gateway to the gatekeeper. In further embodiments, the list of registered DN's is continuously updated.

[0021] The term call is intended to cover calls which convey voice, fax or data. The present invention relates to a multimedia IP line side gateway, preferably having a plurality of ports, e.g. 24 ports ITG Platform hardware, for example providing an H.323 Voice Services Gateway. The multimedia line side gateway according to the present invention may provide the following capabilities:

IP terminal to PSTN calls,
PSTN to IP terminal calls,
direct medium IP to IP calls with signaling via the Line Side Gateway,
direct medium IP to IP calls with signaling via the multimedia IP Line Side and a Trunk Side Gateway,
no double encoding/decoding for basic calls and supplementary services.

[0022] IP Line ports on the ITG card are a shared resource (concentration) within an multimedia switch partition.
[0023] A plurality of IP Line ports per ITG card (e.g. 16 or 24) depending on the required encoding.

voice, fax and modem call are supported. Supported modem protocols include V.21, V.22, V.22bis, V.32, V.32bis and V.34. Fax group 3 is supported as well.
echo cancellation, silence suppression, comfort noise injection

[0024] G.723. 1, G.729, G.729A, G.711 (A and MU laws) standard codecs are supported.
[0025] Address translations, routing, networking are supported.
The following Line Side features are also implemented:

access restrictions
billing capabilities

[0026] On board RADIUS Client for performance statistics.
multi-partition operation on the core switch, ITG cards being exclusive resources for each partition.
[0027] Supplementary services:

call diversion to Voice Mail as well as other destinations
call forward all calls
call forward busy (Hunt)
call forward no answer
call forward not registered
activation of call forward all calls as per H.450.3 Diversion standard
H.450.2 Call Transfer with and without consultation.
CLIP/CLIR
Calling/Connected Name
H.323 Call Waiting

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] Fig. 1 shows an arrangement of an IP telephony gateway in accordance with the present invention.
[0029] Figs. 2A to C, show, respectively, a conventional circuit switched telephone network, a network with IP telephony gateways in accordance with the present invention, and a network with trunk side gateways.
[0030] Fig. 3 is a schematic diagram of an integrated IP telephony gateway in accordance with an embodiment of

the present invention.

[0031] Figs. 4A and B are schematic call routings for a calls involving an IP telephony gateway in accordance with the present invention.

[0032] Fig. 5 is a schematic representation of a network in accordance with an embodiment of the present invention with an IP telephony gateway in accordance with the present invention

[0033] Fig. 6 shows the routing of call components through an IP network in accordance with the present invention when the called and calling IP terminals are in different zones.

[0034] Fig. 7 is a schematic representation of a gateway in accordance with an embodiment of the present invention showing the connections to the ITG cards.

[0035] Fig. 8 is a schematic representation of connections between a core switch and ITG cards in accordance with an embodiment of the present invention.

[0036] Fig. 9. is a schematic representation of modules on an ITG card in accordance with an embodiment of the present invention.

[0037] Fig. 10 is a schematic representation of one way of connecting a gateway in accordance with the present invention and a gatekeeper.

[0038] Fig. 11 shows the protocol layers of a gatekeeper interface in accordance with an embodiment of the present invention.

[0039] Fig. 12 is a schematic representation of the connections between a gatekeeper interface in accordance with an embodiment of the present invention and ITG card modules.

[0040] Figs. 13 to 21 show messaging between gatekeeper and gateway in accordance with embodiments of the present invention.

[0041] Fig. 22 shows call paths for a call between an IP terminal and an SCN terminal for IP network in accordance with an embodiment of the present invention.

[0042] Figs. 23 and 24 show two different call paths for a call between two IP terminals in an IP network in accordance with the present invention.

[0043] Fig. 25 shows call paths for a call between two IP terminals in an IP network in accordance with the present invention when the IP terminals are in different zones.

[0044] Figs. 26 and 27 show message paths for a call between an SCN set and an IP terminal in accordance with an embodiment of the present invention.

[0045] Fig. 28 shows a key for the message flows of Figs. 29 to 34.

[0046] Fig. 29 shows SCN to IP call establishment message flows including an incoming IP to MMCS GW call in accordance with an embodiment of the present invention.

[0047] Fig. 30 shows a message flow for termination ofthe call shown in Fig. 29.

[0048] Fig. 31 shows IP to SCN call establishment message flows in accordance with an embodiment of the present invention.

[0049] Fig. 32 shows IP to IP call establishment message flows in accordance with an embodiment of the present invention.

[0050] Fig. 33 shows a message flow for release of the call shown in Fig. 32.

[0051] Fig. 34 shows IP to IP call establishment message flows in accordance with an embodiment of the present invention when the endpoint IP terminals have different gateways.

[0052] Fig. 35 shows a scheme for a supplementary service in an IP network in accordance with an embodiment of the present invention.

[0053] Fig. 36 is a key for the message flows of Figs. 37 to 41.

[0054] Fig. 37 shows a message flow for call transfer without consultation between two IP clients and an SCN set in accordance with an embodiment of the present invention.

[0055] Fig. 38 shows a message flow for call transfer without consultation between an IP client and two SCN sets in accordance with an embodiment of the present invention.

[0056] Fig. 39 shows a message flow for call transfer without consultation between three IP clients in accordance with an embodiment of the present invention.

[0057] Fig. 40 shows a message flow for call transfer with consultation between three IP clients in accordance with an embodiment of the present invention.

[0058] Fig. 41 shows a message flow for call transfer with consultation between two IP clients and an SCN set in accordance with an embodiment of the present invention

[0059] Fig. 42 shows an H 450.3 message flow for CFAC in accordance with an embodiment of the present invention.

[0060] Fig. 43 shows an H 450.3 message flow for CFAC remote activation in accordance with an embodiment of the present invention.

[0061] Fig. 44 shows the internal message flows for a CFAC remote activation in accordance with an embodiment of the present invention.

Definitions

[0062] A basic call provides communication between two terminal devices of a network over which some form of information may be carried, e.g. voice, data, fax, video.

[0063] A supplementary service is a service which has no existence unless there is an active basic call.

[0064] H.323: ITU-T Recommendation for Packet based multimedia communications systems.

[0065] H.225.0: ITU-T Recommendation for Media Stream Packetization and Synchronization on Non-Guaranteed Quality of Service LANs.

[0066] H.245.0: ITU-T Recommendation for Control protocol for multimedia communication.

[0067] H.450.x: ITU-T Recommendation H.450.1 Line Transmission of non-telephone signals- supplementary services in H.323(.0 Generic functional, .1 call transfer, .2 call diversion)

The following four definitions are H.323 network entities.

[0068] Gateway: this H.323 entity provides an interface between H.323 network and non H.323 network (as the Switched Circuit Network). The present invention is not limited to H323 compliant gateways.

[0069] Gatekeeper: the Gatekeeper (GK) is an H323 entity on the network that provides address translation and controls access to the network for H323 terminals, Gateways, and Multipoint Control Unit (MCU). The present invention is not limited to H3232 compliant gatekeepers.

[0070] IP Client: IP Client is the terminology used in the whole document to name the terminals connected to the IP network (PCs, H.323 Terminal, IP Set, WebPhone, USB phone, or similar).

[0071] Zone: A zone is the collection of all endpoints, e.g. H 323 endpoints (IP Client, GW and MCU) managed by a single gatekeeper. A Zone includes at least one IP client, and may or may not include GW or MCUs.

The following four definitions are related to the core switch.

[0072] Virtual TN (VTN): VTN is a TN representing an IP Client in the core switch. It is used during call processing to handle particular IP Client capabilities and features.

[0073] IPSET: IPSET is used to designate the core switch representation of an IP client.

[0074] Physical TN (PTN): PTN is a TN representing one of the ITG cards ports. It is used during call processing to handle signaling as well as paths. There are preferably less PTNs than IP Clients in a system achieving the required concentration.

[0075] Phantom Loop: this is a type of superloop which is not associated to hardware physically shipped in the core switch. However, it takes resources as if it were a regular superloop. It is used to define IPSETs.

[0076] SCN set: set in the SCN which is not managed by MMCS.

The following two terms are widely used in the document.

[0077] MMCS Gateway: this designates the global IP telephony gateway based on the MMCS platform and made of the MMCS core switch and of the ITG cards.

[0078] ITG: this designates the ITG card itself.

The following three definitions are related to the ITG cards:

[0079] Leader: the leader ITG card is a unique card chosen to be the point of contact for all other ITG cards and for other customers or core switches too. Each leader preferably has to maintain the set of leader/backup leader of other customers or core switches of the network. The leader controls the pool and assignment of IP addresses of its follower cards.

[0080] Backup Leader: the backup leader ITG card is a unique card on a customer chosen to step in when, for some reason, the leader is disabled or out of service. The backup leader ITG card has to keep its database in synchronization with the leader card's database.

[0081] Follower: all ITG cards which are neither leader nor backup leader are named as follower cards.

The following three definitions are related to networks:

[0082] Extranet: it is used to designate a managed IP network engineered for quality IP telephony services (as opposed to internet which refers to the unmanaged IP network).

[0083] ELAN: is the core switch 10Base T LAN used for management and for part of the signaling between the core switch and the ITG.

[0084] Voice LAN: it is the 10/100 Base T LAN used for IP voice signaling between the ITG and the extranet.

The following two definitions are related to IP clients:

[0085] DN: is the digits directory number associated to a VTN in the core switch. It typically has 4 to 7 digits

[0086] E.164 number: it is the number of the IP client following the E.164 standard and allowing to uniquely define the IP client.

Abbreviations	
ATM	Address Translation Module

(continued)

Abbreviations	
API	Application Programming Interface. High level language software used as components in the development of an application.
ARP	Address Resolution Protocol
BCS	Business Communication Set
CDR	Call Detail Recording
CFAC	Call Forward All Calls
CFB	Call Forward Busy
CFNA	Call Forward No Answer
CFNR	Call Forward Not Registered
CFU	Call Forward Unconditional
CLS	CLass of Service
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CS	Core Switch
DRAM	Dynamic Random Access Memory
DN	Directory Number
DID	Direct Inward Dialing
DSP	Digital Signaling Processor
EES	End to End Signaling
EDD	Data Dump
ELAN	Embedded LAN
EPROM	Erasable Programmable Read Only Memory
EXUT	Extended Universal Trunk
FS	Feature Specification
GK	GateKeeper
GW	GateWay
ICDA	Internal CDr Allowed
IE	Information Element
IP	Internet Protocol
IPLC	IP Line Card
IPLL	IP Local Loop
IPLS	IP Line Side
ISDN	Integrated Services Digital Network
ITG	IP Telephony Gateway
ITM	Individual Traffic Measurement
L/BL/F	Leader/Backup Leader/Follower
LAN	Local Area Network

(continued)

Abbreviations	
MAT	Meridian Administration Tool. Windows 95 application used for configuring the Meridian 1 and MMCS switch.
MIX	Meridian Integrated XoiP
MMCS	Multimedia Carrier Switch
MWI	Message Waiting Indication
NPM	Network Protocol Module
NTP	Northern Telecom Publication.
OA&M	Operations, Administration and Maintenance
OS	Operating System
PBX	Private Branch eXchange. A telephony switch that is privately owned.
PSTN	Public Service Telephony Network
PTN	Physical TN
QOS	Quality Of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Remote Function Call OR Request For Comment
RM	Resource Manager
SCN	Switched Circuit Network
SNMP	System Network Management Protocol
SSD	Scan and Signal Distributor
TBD	To Be Determined
TCP	Transmission Control Protocol
TN	Terminal Number
TSGM	Telephony SignallinG Module
UDP	User Datagram Protocol
USB	Universal Serial Bus
UUIE	User to User IE
VPS	Voice Processor System
VTN	Virtual TN
WAN	Wide Area Network
XoIP	Voice or Fax over IP
XDLC	Extended Digital Line Card.
XPEC	Expanded Peripheral Equipment Controller Pack

DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

[0087] The present invention will be described with reference to certain embodiments and drawings but the present invention is not limited thereto but only by the claims. In particular the present invention will be described with reference to the H 323 suite of standards but the present invention is not limited thereto.

[0088] As shown schematically in Fig. 1 an IP Telephony gateway in accordance with the present invention provides a bridge between a circuit switched network and voice services based on an IP network and technology. A basic call originating from a PSTN telephone and terminating on an H.323-based terminal in an IP network is directed to the

appropriate IP Telephony Gateway. This gateway performs the following minimum functions:

- translates between transmission formats
- terminates the PSTN signaling protocol and bearer channel
- terminates the H.323 signaling protocols and bearer channel
- provides bearer interworking facilities from the PSTN format (typically 64kbs PCM) to the appropriate IP bearer format implemented on the specific network (typically one of several compressed voice standards listed in the H. 323 specifications).
- translates between communication procedures
- manages the PSTN-side call processing and signaling
- locates the correct H.323 gatekeeper for the called party
- originates and manage an H.323 call to the appropriate gatekeeper

A basic call originating from an H.323 terminal and terminating on a PSTN telephone would be handled in the same way in the other direction.

[0089] In some embodiments of the present invention the gatekeeper translates between addressing formats and domains. In accordance with the present invention the gateway and gatekeeper functionality can be integrated together into a single unit if needed to simplify deployment in applications such as toll arbitrage.

[0090] In support of the initial services envisioned for IP Telephony, IP gateways can appear both on the trunk side and on the line side of a circuit switch such as the MMCS.

[0091] A Trunk-side Gateway (Fig. 2C) enables a circuit switched central office switch to route inter-switch traffic via IP data networks, bypassing circuit switched trunk facilities.

[0092] A Line-side Gateway 2, 6 (see Fig. 2B) enables a circuit switched central office switch 4, 5 to provide line-side services to terminals 7, 8 deployed on IP data networks 1, 3 (i.e. IP-based replacement of the subscriber loop access).

[0093] An gateway 6 may provide additional call processing services under the control of either an H.323 gatekeeper or a circuit switched office when the Gateway 6 is integrated with a feature rich switch 5, as is the case with embodiments of the present invention involving as it does an MMCS Gateway.

[0094] The gatekeeper can play an important central role by routing all call control messaging through it and by using the gatekeeper to provide services such as pre-paid billing, call forwarding leaving the gateways as only protocol. translators The potential advantages of such a Gatekeeper-Centric Architecture are:

- Simplified service provisioning
- Simplified configuration management
- Centralized billing
- Open APIs for 3rd party service development
- Single interface point to PSTN IN/AIN
- Single service implementation, accessible to all Gateways
- Lower Gateway intelligence -> cheaper Gateways?
- Faster time to market for new services?

Potential Disadvantages of a Gatekeeper-Centric Architecture are:

- Gatekeeper is single point of failure
- Scalability - network signaling, Gatekeeper processor
- Handling of feature interactions
- Handling of race conditions
- Time to market of initial service offerings

The IP-networks and gateways in accordance with the present invention exploit the advantages of a Gatekeeper-centric architecture while addressing the issues of the centralized Gatekeeper approach.

[0095] Applications can be segmented into backhaul applications which utilize IP Trunks and access applications which utilize IP Lines. IP Telephony backhaul and access applications can be offered separately or combined by carriers into a service which utilizes both IP Trunk and IP Line capabilities. The present invention includes several IP trunk backhaul and IP Line access applications.

[0096] Corporations typically have separate connections for voice communications for data communications. IP Telephony provides a means for corporations to aggregate all of those connections into a single pipe to achieve savings in connectivity fees. IP Line access applications offer line side services over IP Telephony transport. IP Telephony as

an alternative to twisted pair loop technology has value even in cases where it is only utilized in the local loop, with the circuit switched network is still being used for backhaul of the traffic to the destination point in the case of IP Line originated calls, or from the origination point in IP Line terminated calls.

[0097] A "virtual second line" utilizes IP Telephony to enable subscribers to be on-line (i.e. have a computer connection to an ISP) while making or receiving voice calls via IP Telephony. A growing number of corporate workers are bringing work home from their office/place of business occasionally after work and on weekends. Many of these workers may need to access their corporate data network to send and receive e-mail, download and upload files, and to access their corporate Intranet or the Internet. If they don't have a second line, they will tie up the family phone while they are on-line to the office. If the worker works part of the work day at home on a casual basis during business hours, the virtual second line will enable him/her to make calls to co-workers while on-line. Home based employees want all of the best residential services and all of the best business services, integrated but separable into small packages at a reasonable price. The business services can be accessed either via a dial up modem connection or an xDSL (or other high speed) connection. The IP Telephony voice line using the gateway and IP network in accordance with the present invention can provide services such as Conference, Transfer, Hold, Message Waiting, Voicemail Access, Class of Service, and private dialing plans.

[0098] "Road Warriors" are typically employees of corporations that need access to their corporate networks on a casual or roaming basis. Small Office Home Office (SOHO) subscribers may require their office to move with them (nomadic voice and data) as they move between business locations. In the case of the corporate Road Warrior, voice services delivered to the remote user will encompass the desktop capability that a featured set at the office would have such as Conference, Transfer, Hold, Message Waiting, Voicemail Access, Class of Service, and private dialing plans.

[0099] Phones which are part of a MADN group all ring simultaneously when an incoming call is presented to the pilot directory number of the MADN group. Any phone in the MADN group can answer the call. Once the call is answered, all phones in the MADN group stop ringing. This capability can be used in various situations in which multiple phones should ring when a call is presented to a pilot directory number. For example, executives typically have the directory number of their desk phone programmed into a MADN group with their secretary such that the secretary can screen incoming calls. MADN functionality has also been implemented on Service Node platforms to provide a network wide MADN as a "personal number service" in which multiple phones on separate switches can be rung simultaneously when a call is presented to a pilot directory number. However, one major disadvantage of a Service Node-based network wide MADN is that it is expensive to deploy since trunks are tied up to/from the Service Node as well as across the network to the phone that answers the call. In accordance with the present invention IP Telephony can be used to achieve the functionality of both a localized MADN as well as a network wide MADN by using IP Telephony Clients combined in conjunction with the MADN capabilities of the MMCS Gateway. IP Telephony is a much more cost effective approach to network wide MADN since remote IP Telephony Clients can be part of a MADN group without tying up expensive trunk facilities.

[0100] An MMCS Gateway 10 in accordance with an embodiment of the present invention is shown schematically in Fig. 3. It comprises a core switch 24 combined with gateway (ITG) cards 22. The main advantages of the integrated Gateway 10 versus stand-alone adjunct systems are:

1. Cost improvement
2. Integrated OA&M
3. Seamless integration of circuit switched and IP environments -- call processing and OA&M

The MMCS Gateway 10 can achieve the cost improvements and integrated OA&M benefits by integrating the IP Telephony Gateway (ITG) into the MMCS platform. In addition, the MMCS Gateway 10 achieves a more seamless integration ofthe circuit switched and IP networks by tightly coupling the MMCS core switch 24 with the IP Telephony Gateway 22. A call moves seamlessly between the circuit switched and IP environments during the course of the call to handle call setup, tear down, and mid-call features.

[0101] Figs. 4A and B demonstrate certain call scenarios supported by embodiments of the present invention. The call scenarios are identified by the numbers 1 through 5. With the network of Fig. 4A

1. Call Scenarios: (a) PSTN to IP Telephony Client 16, 18 through Home Gateway 10, (b) IP Telephony Client 16, 18 to PSTN through Home Gateway 10. The IP Telephony Client 16, 18 will appear as an "IP Line" on incoming calls from the PSTN and calls outgoing to the PSTN through the Home Gateway 10.

2,3. Call Scenario: All originating calls from an IP Telephony Client are sent to its Home Gateway 10 for processing. If the call is routed by the MMCS 24 back to the IP network 12 to either a Remote Gateway, or another IP Telephony Client, the MMCS 24 will instruct the Gateway cards 22 involved to bypass the G.7xx vocoders ("vocoder bypass") such that the call does not encounter a double encode/decode of the voice and hence suffer voice quality degra-

appropriate IP Telephony Gateway. This gateway performs the following minimum functions:

- translates between transmission formats
- terminates the PSTN signaling protocol and bearer channel
- terminates the H.323 signaling protocols and bearer channel
- provides bearer interworking facilities from the PSTN format (typically 64kbs PCM) to the appropriate IP bearer format implemented on the specific network (typically one of several compressed voice standards listed in the H. 323 specifications).
- translates between communication procedures
- manages the PSTN-side call processing and signaling
- locates the correct H.323 gatekeeper for the called party
- originates and manage an H.323 call to the appropriate gatekeeper

A basic call originating from an H.323 terminal and terminating on a PSTN telephone would be handled in the same way in the other direction.

[0089] In some embodiments of the present invention the gatekeeper translates between addressing formats and domains. In accordance with the present invention the gateway and gatekeeper functionality can be integrated together into a single unit if needed to simplify deployment in applications such as toll arbitrage.

[0090] In support of the initial services envisioned for IP Telephony, IP gateways can appear both on the trunk side and on the line side of a circuit switch such as the MMCS.

[0091] A Trunk-side Gateway (Fig. 2C) enables a circuit switched central office switch to route inter-switch traffic via IP data networks, bypassing circuit switched trunk facilities.

[0092] A Line-side Gateway 2, 6 (see Fig. 2B) enables a circuit switched central office switch 4, 5 to provide line-side services to terminals 7, 8 deployed on IP data networks 1, 3 (i.e. IP-based replacement of the subscriber loop access).

[0093] An gateway 6 may provide additional call processing services under the control of either an H.323 gatekeeper or a circuit switched office when the Gateway 6 is integrated with a feature rich switch 5, as is the case with embodiments of the present invention involving as it does an MMCS Gateway.

[0094] The gatekeeper can play an important central role by routing all call control messaging through it and by using the gatekeeper to provide services such as pre-paid billing, call forwarding leaving the gateways as only protocol. translators The potential advantages of such a Gatekeeper-Centric Architecture are:

- Simplified service provisioning
- Simplified configuration management
- Centralized billing
- Open APIs for 3rd party service development
- Single interface point to PSTN IN/AIN
- Single service implementation, accessible to all Gateways
- Lower Gateway intelligence -> cheaper Gateways?
- Faster time to market for new services?

Potential Disadvantages of a Gatekeeper-Centric Architecture are:

- Gatekeeper is single point of failure
- Scalability - network signaling, Gatekeeper processor
- Handling of feature interactions
- Handling of race conditions
- Time to market of initial service offerings

The IP-networks and gateways in accordance with the present invention exploit the advantages of a Gatekeeper-centric architecture while addressing the issues of the centralized Gatekeeper approach.

[0095] Applications can be segmented into backhaul applications which utilize IP Trunks and access applications which utilize IP Lines. IP Telephony backhaul and access applications can be offered separately or combined by carriers into a service which utilizes both IP Trunk and IP Line capabilities. The present invention includes several IP trunk backhaul and IP Line access applications.

[0096] Corporations typically have separate connections for voice communications for data communications. IP Telephony provides a means for corporations to aggregate all of those connections into a single pipe to achieve savings in connectivity fees. IP Line access applications offer line side services over IP Telephony transport. IP Telephony as

an alternative to twisted pair loop technology has value even in cases where it is only utilized in the local loop, with the circuit switched network is still being used for backhaul of the traffic to the destination point in the case of IP Line originated calls, or from the origination point in IP Line terminated calls.

[0097] A "virtual second line" utilizes IP Telephony to enable subscribers to be on-line (i.e. have a computer connection to an ISP) while making or receiving voice calls via IP Telephony. A growing number of corporate workers are bringing work home from their office/place of business occasionally after work and on weekends. Many of these workers may need to access their corporate data network to send and receive e-mail, download and upload files, and to access their corporate Intranet or the Internet. If they don't have a second line, they will tie up the family phone while they are on-line to the office. If the worker works part of the work day at home on a casual basis during business hours, the virtual second line will enable him/her to make calls to co-workers while on-line. Home based employees want all of the best residential services and all of the best business services, integrated but separable into small packages at a reasonable price. The business services can be accessed either via a dial up modem connection or an xDSL (or other high speed) connection. The IP Telephony voice line using the gateway and IP network in accordance with the present invention can provide services such as Conference, Transfer, Hold, Message Waiting, Voicemail Access, Class of Service, and private dialing plans.

[0098] "Road Warriors" are typically employees of corporations that need access to their corporate networks on a casual or roaming basis. Small Office Home Office (SOHO) subscribers may require their office to move with them (nomadic voice and data) as they move between business locations. In the case of the corporate Road Warrior, voice services delivered to the remote user will encompass the desktop capability that a featured set at the office would have such as Conference, Transfer, Hold, Message Waiting, Voicemail Access, Class of Service, and private dialing plans.

[0099] Phones which are part of a MADN group all ring simultaneously when an incoming call is presented to the pilot directory number of the MADN group. Any phone in the MADN group can answer the call. Once the call is answered, all phones in the MADN group stop ringing. This capability can be used in various situations in which multiple phones should ring when a call is presented to a pilot directory number. For example, executives typically have the directory number of their desk phone programmed into a MADN group with their secretary such that the secretary can screen incoming calls. MADN functionality has also been implemented on Service Node platforms to provide a network wide MADN as a "personal number service" in which multiple phones on separate switches can be rung simultaneously when a call is presented to a pilot directory number. However, one major disadvantage of a Service Node-based network wide MADN is that it is expensive to deploy since trunks are tied up to/from the Service Node as well as across the network to the phone that answers the call. In accordance with the present invention IP Telephony can be used to achieve the functionality of both a localized MADN as well as a network wide MADN by using IP Telephony Clients combined in conjunction with the MADN capabilities of the MMCS Gateway. IP Telephony is a much more cost effective approach to network wide MADN since remote IP Telephony Clients can be part of a MADN group without tying up expensive trunk facilities.

[0100] An MMCS Gateway 10 in accordance with an embodiment of the present invention is shown schematically in Fig. 3. It comprises a core switch 24 combined with gateway (ITG) cards 22. The main advantages of the integrated Gateway 10 versus stand-alone adjunct systems are:

1. Cost improvement
2. Integrated OA&M
3. Seamless integration of circuit switched and IP environments -- call processing and OA&M

The MMCS Gateway 10 can achieve the cost improvements and integrated OA&M benefits by integrating the IP Telephony Gateway (ITG) into the MMCS platform. In addition, the MMCS Gateway 10 achieves a more seamless integration ofthe circuit switched and IP networks by tightly coupling the MMCS core switch 24 with the IP Telephony Gateway 22. A call moves seamlessly between the circuit switched and IP environments during the course of the call to handle call setup, tear down, and mid-call features.

[0101] Figs. 4A and B demonstrate certain call scenarios supported by embodiments of the present invention. The call scenarios are identified by the numbers 1 through 5. With the network of Fig. 4A

1. Call Scenarios: (a) PSTN to IP Telephony Client 16, 18 through Home Gateway 10, (b) IP Telephony Client 16, 18 to PSTN through Home Gateway 10. The IP Telephony Client 16, 18 will appear as an "IP Line" on incoming calls from the PSTN and calls outgoing to the PSTN through the Home Gateway 10.

2,3. Call Scenario: All originating calls from an IP Telephony Client are sent to its Home Gateway 10 for processing. If the call is routed by the MMCS 24 back to the IP network 12 to either a Remote Gateway, or another IP Telephony Client, the MMCS 24 will instruct the Gateway cards 22 involved to bypass the G.7xx vocoders ("vocoder bypass") such that the call does not encounter a double encode/decode of the voice and hence suffer voice quality degra-

dation. Note that the terminating IP Telephony Client 16, 18 my have another Home Gateway, and hence, the call may pass through two MMCS Gateways with the vocoders being bypassed.

4. Call Scenario: PSTN to Voice Mail (VMS) - this is an extension to call scenario 1. When a call forwarding condition is detected (Call Forward Busy, Call Forward No Answer, Call Forward Unconditional), the incoming PSTN will be forwarded to a voice mail system attached to the MMCS Gateway 10. Note: The forwarding destination is dependent on the programming of the call forwarding number and hence, does not have to be to voice mail.

5. Call Scenario: Because all calls from an IP Telephony Client 16, 18 pass through the Home Gateway 10, the call forwarding treatment of a call to an IP Telephony Client 16, 18 will be implemented by the call forwarding service logic of that IP Telephony Client's MMCS Home Gateway 10.

Although architecture of Fig. 4A enables access to the MMCS Gateway line side services in all call scenarios without degrading voice quality, the architecture has the disadvantage of tying up two Gateway ports for IP Telephony Client originated calls which terminate back into the IP network 12 either to another IP Telephony Client 16, 18 or to a Remote Gateway 10'. A more ideal situation would be to have the voice packets transmitted directly between the originating IP Telephony Client and the other IP Telephony end point with only the call control signaling passing through the MMCS Gateway 10. This would free up the MMCS Gateway ports for calls to/from the PSTN and is shown in Fig. 4B. In this architecture, the MMCS would play the role of an IP Telephony Gateway for calls to/from the PSTN as well as the role of a call processing server off the IP network 12. The MMCS Gateway 10 server functionality would be similar to that envisioned for an H.323 Gatekeeper under a gatekeeper-routed calls paradigm. For Fig. 4B:

1. Call Scenario: Same as for Fig. 4A.

2,3. Call Scenario: All originating calls from an IP Telephony Client 16, 18 are sent to its Home Gateway 10 for processing. If the call is routed by the MMCS 10 back to the IP network 12 to either a Remote Gateway 10', or another IP Telephony Client 18, 16, the MMCS 10 will instruct the IP Telephony Client 18, 16 to establish the voice path directly to the other IP Telephony end point 16, 18 while continuing to send the call signaling information to the MMCS 10.

4. Call Scenario: Same as for Fig. 4A.

5. Call Scenario: Because the call control signaling for all from an IP Telephony Client 16, 18 passes through the Home Gateway 10, the call forwarding treatment of a call to an IP Telephony Client 16, 18 will be implemented by the call forwarding service logic of that IP Telephony Client's MMCS Home Gateway 10.

The Gatekeeper 10 can comprise the following functions:

1. IP and E164 mapping for trunk operation and for line side access for IP devices on remote Gateways (in another free-calling area) using E164 as the mediation numbering plan for mediation across the network.
2 IP and E164 mapping service for IP to IP calls.
3. Interactive communication with the MMCS Gateway to be able to provide the proper IP address to external devices (remote gateway or local/remote IP device) for gateway access.
4. Registration of IP devices associated with a home gateway and managing current temporary IP addresses of the devices registered for mapping purposes.
5. Authentication that the user registering an IP device is an authorized user.

Other functions may also include:

1. For IP device to IP device communications, the gatekeeper should immediately forward a call for 'call treatment' to the IP device's home gateway once it has it has it been determined that the terminating IP device is 'not registered'.
2. Usage billing data for IP to IP device communications. The usage fee would be for the use of the 'managed IP extranet', an enhanced service over the 'free or general internet'.
3. Gatekeeper to Gatekeeper synchronization.
4. High level 'Root - DNS' - like server or Voice DNS (VDNS) maps E164 ranges to associated gateways in 'free calling areas'.

[0102] The Gateway 10 discriminates between voice, fax and data calls on a call by call basis and handles each appropriately. The solution should not be dependent upon the served PBX or VPN being configured with service specific numbers, and it should be possible to seamlessly detect the initiation and completion of a fax transaction during a voice call. The MMCS Gateway should be able to transport and receive the following media over the IP network:

Voice: The following encoding schemes are supported at a minimum: G.729A: G.723.1; G.711 u-law; G.711 A-law. The gateway 10 is able to dynamically change the codec used on a call by call basis.

DTMF: Voice calls traversing the gateways 10 are able to faithfully detect and relay in-band DTMF signals.

Echo Suppression: Echo suppression conforms to acceptable industry standards for quality echo suppression in the circuit switched network.

Silence Suppression: The IP Telephony codecs support silence suppression.

Noise Suppression: The IP Telephony codecs support noise suppression.

*Flexible Dialing Plans:*North American Numbering Plan, International Numbering Plan, and VPN numbering plan support.

Network Class of Service: Provides a means to control access to Gateway routes. Enables carriers to flexibly define QoS packages such as a "Take what you get" low cost/low QoS, a "Guaranteed" high cost/high QoS, and a "Selectable on a call by call basis" pay for QoS selected.

Call Forwarding: The MMCS Gateway 10, in conjunction with the Gatekeeper 20 supports all forms of call forwarding: Call Forward Busy (CFB), Call Forward No Answer (CFNA), and Call Forward Unconditional (CFU). As well, an additional type of call forwarding called "Call Forward Not Registered" (CFNR) is provided, since IP Telephony Clients will not always be registered or reachable.

Call Forward Not Registered: The CFNR feature uses the same destination as the CFNA feature. When an IP Telephony Client for an incoming call is not registered with the Gatekeeper, the call should be forwarded to the CFNA destination if one is programmed for the subscriber. If a CFNA destination has not been programmed, then the incoming call should receive an appropriate treatment.

Line-side Alternate Routing: When an IP Line is unavailable for termination due to Gateway card overload, network congestion, etc., the call should be treated as if the subscriber is not registered (i.e. the subscriber is not reachable) and the call is forwarded using the CFNA treatment. If the subscriber does not have CFNA, then the call is routed to an appropriate treatment.

Call Forward Directory Numbers: Call forwarding directory numbers may be stored in the subscriber line data in the MMCS Gateway 10. IP Line subscribers are able to access and program the call forwarding directory numbers via their IP Telephony Client interface.

Terminating Restrictions: An IP Telephony carrier is able to setup an IP Line such that call terminations to the IP Line are denied.

Originating Restrictions: When setting up an IP Line, an IP Telephony carrier has the following options in restricting the types of originations made from the Line:

Denied Origination: The IP Line is not allowed to originate any calls.
Local Calls Only: The IP Line is not allowed to originate calls outside the free calling area.

Local and North American LD: The IP Line is allowed to originate all types of calls excepts for International long distance.

Local, North American LD, International LD: The IP Line is allowed to originate all types of calls.

Selective Number Screening (e.g. 976, 900): The IP Line is restricted from originating calls to selected numbers.

[0103] The requirements particularly for a corporate road warrior service are as follows:

Single Directory Number: A corporate road warrior has one directory number on his/her business card that callers can use to reach the road warrior, regardless of whether he/she is at the office or on the road.

Single Voice Mail Box: The road warrior is able to have all calls forwarded to the same voice mail box, regardless of whether the incoming call attempted to terminate to an office phone or to an IP Telephony Client. The road warrior has the option of using the Voice Mail System off a PBX, Centrex Central Office, or MMCS Gateway to provide the single voice mail box.

Reachability: The corporate road warrior service is able to reach the subscriber on an IP Telephony Client while the road warrior is out of the office traveling or at home, and on a desk phone while the road warrior is in the office.

Subscriber Transparency: The corporate road warrior service operates transparently to the subscriber. For example, the subscriber does not have to manually activate call forwarding from his/her desk phone to the IP Telephony Client when he/she leaves the office.

[0104] An embodiment of the integrated telephony gateway in accordance with present invention will be described in the following in detail. An ITG in accordance with this embodiment of the present invention emulates an analog trunk based gateway providing the ability to network switches such as Meridian 1 switches provided by Nortel networks, Canada while transmitting signaling and voice over an IP network. As shown schematically in Fig. 5, the integrated MMCS Line Side gateway 10 provides communications between a first network, which may be a Switched Circuit Network (14) such as a PSTN or an enterprise network 15 and a plurality of Clients 16, 18 connected on a IP Network which is preferably a managed IP network (extranet) 12 with controlled delays and quality of service (QoS). The enterprise network 15 and the SCN 14 may communicate with the gateway 10 over ISDN lines. The clients 16, 18 are preferably H323 compatible clients but the present invention is not limited thereto. Clients 16, 18 may be personal computers, workstations or telephone sets especially adapted to use IP telephony. The line side gateway 10 handles SCN calls to/from IP clients 16, 18 as well as IP client to IP client calls. The gateway 10 also communicates with another entity, the gatekeeper 20, mainly for control access, IP client registration and monitoring. The gatekeeper 20 may be H323 compliant but the present invention is not limited thereto. An ITG card device 22 on the gateway 10 is an interface processing voice and fax coming from the core switch 24 and the IP based packet network 12. Gateway 10 may be linked to trunk side gateway operation or may have such functionality integrated therein. Calls coming from one IP zone and going to another IP zone typically involve both line side and trunk side gateway operation.

[0105] The ITG (MIX) line side emulates an XDLC line card. The ITG (MIX) Gateway 10 assumes the customer has already installed a corporate IP network 12 and that routers are available for any WAN connectivity between networked systems, e.g. Meridian systems frim Nortel Networks, Canada. The configuration preferably includes 10/100 Base T Ethernet interfaces and support of the IP version 4 or 6 layer and addressing in a WAN. No restriction is anticipated on the physical medium on the WAN. If an H.323 FastConnect procedure is used during call establishment, tone is provided to the calling IP Client 16, 18 by the SCN 14 when the calling IP Client 16, 18 is alerting. In other cases, tones (or any means to represent tones on an IP client) are generated by the IP client 16, 18 itself In fact, at the time when tones need to be heard, there is no path established between the MMCS gateway 10 and the IP client 16, 18 and then, the IP client 16, 18 is not able to hear the tones provided by the MMCS gateway 10. The ITG cards 22 are preferably organized into leader and follower cards. All follower cards register to the Gatekeeper 20. Voice LAN is engineered so that all ITG cards 22 can have simultaneous calls without bandwidth shortage. It is also assumed that the IPLL Gatekeeper 20 provides routed call signaling, supports messaging for valid DN upload, accepts DNs of up to 10 digits and forwards set status to gateway 10.

[0106] Fig. 6 shows schematically the signaling path of an IP client call from one zone to another IP client belonging to another zone. In this case two local gatekeepers 20 and 20' and two gateways 10, 10' are involved with an IP network 12 between having a network gatekeeper 26. A suitable message sequence may be:

(1) The call generated by IP client 16 is first routed to the MMCS 10 by the local GK 20 of client 16. In accordance with the present invention several ways of accessing the gatekeeper/gateway are possible. As alternatives, the call may be routed to the gateway 10 which then communicates with the gatekeeper 20 to obtain authorization of the call. Yet another alternative is that the call may first be routed to the gatekeeper which provides authorization. After receiving this, client 16 the begins setting up the call with gateway 10.
(2) The line side GW card 22 of the gateway 10 passes the call to the Core Switch 24 which processes it and re-routes it to an IP trunk ITG card 25. ITG trunk card 25 may be integrated with gateway 10.
(3) The trunk side IP GW determines that the call terminates on MMCS gateway (GW) 10'. The call is directly

routed to MMCS GW 10' through the IP network 12.

(4) The trunk side card 25' of IP GW 10' transmits the call to the Core Switch 24' of gateway 10' which processes it and places it to the Line side ITG card 22'.

(5) The call is eventually routed by the Line Side GW 10' to IP client 18 via its local GK 20'.

[0107] Fig. 6 shows a possible schematic arrangement of the ITG (MIX) cards 22-1, 22-2, 22-3 within the gateway architecture. The ITG emulates an XDLC card and communicates to the core switch software via the DS-30X link 36. Two Ethernet ports may be available on each card 22-1, 22-2, 22-3. One port 38 (10/100 BaseT) is used for the IP voice signaling whereas the other one 39 is used as an interface with a MAT station 40 for management purpose as well as for a communications link between ITG cards 22-1, 22-2, 22-3.

[0108] For each customer data block defined on a core switch 24, there is one set of leader, optional backup leader and follower cards 22-1, 22-2, 22-3, which are available to that customer only. As the ITG cards 22-1, 22-2, 22-3 are VPS cards which emulate a Digital Line card (XDLC), IP Clients 16, 18 are represented in the Core Switch 24 by a BCS set (**IPSET**). Each IP client IPSET is identified by a Virtual TN (VTN) which is defined on a phantom loop. For each IP VTN involved in a call, an available TN on the ITG card is dynamically associated to this VTN in order to access this card. This TN, called the Physical TN (PTN) is only used for signaling (through Ethernet and SSD) and for speech-path between the Core Switch 24 and the ITG card 22-1, 22-2, 22-3. The IP Client capacities and the call processing is associated to its VTN. One aspect of the present invention is that the client profile is defined by the VTN and is dynamically linked to the call using the PTN at call set-up. This VTN/PTN mechanism permits definition of more IP Clients than physical resources (i.e. PTN) and hence allows pooling of PTN resources.

[0109] As an IP Client 16, 18 may support several simultaneous active "calls" on the same DN, an IP Client 16, 18 can be composed by several IPSETs (i.e. by several VTNs) which have the same DN. Preferably, each VTN has a single DN and all the VTNs which have the same DN are IPSET. For each call to a DN only one VTN is concerned. In case of a call to IP, when the called DN has several VTNs, the Core Switch 24 chooses one VTN which is idle and presents the call to the ITG card 22-1, 22-2, 22-3 for only this VTN. In case of a call from IP, when the calling DN has several VTNs, the Core Switch 24 chooses one VTN which is idle and all the call processing is done with this VTN. As an IP Client 16, 18 may support several call types (e.g. 2 data calls, a fax and a voice call), an IP Client 16, 18 can be composed by several IPSETs.

[0110] Preferably, an IP Client 16, 18 has to register on the Gatekeeper 20 before initiating or receiving a call. A new Registration / Unregistration state is introduced in the Core Switch 24 for each IPSET. This state is updated in the Core Switch 24 by message sent from the Gatekeeper 20 each time an IP client 16, 18 gets registered or unregistered. When the called IPSET is not registered, the call is immediately treated in such a way that resources are not reserved or used. For, example, the call may be diverted to a HUNT DN, as explained later.

[0111] Communications between the Core Switch 24 and the ITG cards 22 are done through a suitable signaling protocol and hardware, e.g. Ethernet and/or SSD signaling. As the ITG card 22 emulates an XDLC card, SSD signaling is also used for IP Clients 16, 18. However, IP Clients 16, 18 require more messaging which cannot be easily handled by the SSD signaling. For instance, when a call is initiated to an IP Client 16, 18 the core switch 24 requests the Leader ITG card to provide a physical TN. The SSD signaling is not adapted to this kind of messaging. So, a connection through Ethernet (UDP) between the Core Switch 24 and the ITG cards handles this messaging.

[0112] Fig. 8 on page 34 shows the two signaling paths for the communications between the Core Switch 24 and ITG cards 22-4, 22-5, 22-6. Messages that cannot be sent through the SSD route 41 are sent through another route such as an Ethernet route 47. A module 44 is the interface between the SL1 task 42 and the UDP/IP API 45, 46 from VxWorks 48. When VoIP is configured, a new task is spawned by the module 44 on the core switch 24. This task is responsible for reading the messages coming from the UDP pipe.

[0113] To send messages to a card 22-4, 22-5, 22-6 the SLI task 42 communicates directly with this module 44 through an interface handler 49. When a message from a card 22-4, 22-5, 22-6 is received by the module 44, it informs the SL I task 42 via an RFC call.

The task can start up in two ways:

Cold Start if the database has VoIP line side configured

Service Change when a craftperson configures VoIP line side

The ITG operation is separated into distinct areas, each fitting one of the functionalities required from the ITG card 22. The ITG gateway software architecture is divided into two main components, the DSP component 32 (Fig. 7) responsible for processing the voice and FAX data from the core switch 24 and the IP based packet network, and the host component 34 responsible for interfacing with the core switch 24 and the IP network 12. Fig. 9 illustrates the different modules of the host component 34.

[0114] A Network Management Module 52 is responsible for communications between the ITG card 22 and the

craftsperson. The connection can be made over ethernet or serial. The client applications available to the craftsperson for access to the ITG card 22 can be a PC running MAT, a telnet session, or a serial link. An SNMP agent is used to generate traps to indicate events on the ITG card 22.

[0115] An Elan Signaling Module 54 handles messaging to and from the core switch 24 by using the ELAN connection 30. It connects with a 10-baseT ethernet driver to access the ELAN, to relay messages to/from the network protocol module 53 so as to interact with the core switch call processing. It also connects with the resource management (51) on the leader card 22-4 to transmit the requests from the core switch 24 to obtain a physical TN assigned to a call going out on the IP network 12, and their responses. The module 54 is also responsible for interfacing Leader/ Backup-Leader card and Followers of different modules. Communication is mainly needed between the Resource Management module 51 of the Leader card 22-4, and the Network Protocol Module 53 of Follower cards 22-5, 22-6 for the first one to provide the second one with call processing information (PTN, IP address ofGK, UUI IE...). At restart time, and in case of warm/cold start on the core switch 24, this module 54 is in charge of reestablishing the connection between Core Switch 24 and Leader Card 22-4. This module 54 operates on all ITG cards 22.

[0116] The Network Monitoring module 55 is in charge of assessing the conditions on the ethernet segment on which the ITG card 22 is located. First, the vxWorks IP and TCP stacks gather some statistics for each interface, which can indicate a degraded condition, such as loss of packets and other measurements. Alternately, by periodically sending RTCP messages to pre-determined hosts (the gatekeeper 20, the local IP router 33) an estimation of LAN load can be made. Whether this module 55 sits only on the leader 22-4, or on all cards 22, depends on whether the total gateway 10 needs to be located on one or several LAN segments. If several LAN segments are allowed, then several ITG cards 22 need to have this module active (at least one per LAN segment).

[0117] A Resource Management module 51 is responsible for managing system/network resource for the ITG XoIP platform and serves as Gateway to the H.323 network. The system monitor audits ITG card/ channel status. Below is a summary of the Resource Manager task responsibilities:
Address translation interface. This is only required when an Address translation module 59 is present. It only applies to outgoing call s for the leader card 22-4 to interface with the address translation module 59 and retrieve the end-point network address. Resource Control and Maintenance: this functionality contains a set of operations such as:

Task initialization (registration with leader, with MAT...)
Housekeeping (Channel Status Table maintenance)
L-BL Switchover operation
L-BL Database synchronization
Channel Allocation of Incoming and outgoing calls (Leader only)
Call processing information provision to Followers (Leader only)

The same channel allocation algorithm may be applied for outgoing calls as for incoming calls (the core switch 24 is not seizing a trunk but dealing with a virtual DN) and modify it in such a way that only Follower cards 22-5, 22-6 can be chosen to handle a call. This unloads Leaders and Backup-Leaders from some responsibilities generated by the Physical TN selection operation (on core switch request through Ethernet). This can be configurable depending on the system capacity. For systems including a restricted number of ITG cards 22, Leader and Backup-Leader may be configurably to handle calls to prevent reducing traffic capacity which would lead to numerous call rejections.
The resource manager module 51 stores a table providing current allocation of channels, Table 1

Table 1:

Channel Table		
	Possible value	Initialization Value
IP follower:port	IP v4/v6 address:channel	NULL
Status	Idle Reserved Busy Disabled	Idle
Reservation Time	Time Stamp	0
Physical TN		NULL
callRef	cf H.323	NULL
callId	cf H.323	NULL

Where:

IPFollower:port corresponds to a channel of a follower card.
Status corresponds to the use of a follower card channel. *'Idle'* means that no call is going on for that channel. *'Reserved'* means that Gatekeeper has sent a request to make call on that channel but the call is not yet going on. *'Busy'* means that a call is going on for that channel. *'Disable'* is used for maintenance (channel cannot accept call for the time being).
For outgoing calls (CS to IP), the reservation status changes directly from *'Idle'* to *'Busy'* as soon as a physical TN is granted.
For incoming calls (IP to CS), the Leader Card receives a request from the Gatekeeper, allocates a physical TN for the call and then changes reservation status from *'Idle'* to *'Reserved'* for the corresponding channel. The time of the request is also stored. Reservation Status is set to *'Busy'* when the follower card acknowledges that it has received an incoming call.
Reservation Time - this time corresponds to when a physical TN is granted. It is used as a timeout marker when TN allocation is made. If the physical TN is marked as reserved and time stamp is too old, the physical TN is re-allocated. This field is ignored if reservation status is different from *'Reserved'*.
Physical TN - this is the TN allocated by the Resource Management module 51 and used by the Core Switch to send X11 messages.
callRef- this information is used to link incoming calls with outgoing calls.
callId - this information is defined by H.323 standard and identify a call.
Search on this table can be made by: Channel, PTN or callRef

[0118] A Telephony Module 56 handles the receiving and sending of SSD messages according to the state of the H.323 call handled by the Network Protocol module 53. It interfaces with the XDLC emulation to retrieve SSDs and provides an API to the network protocol to receive and send these. It communicates with the network protocol module 53 to transmit and receive SSD messages, and operates on all ITG cards 22.

[0119] On each ITG card 22, instead of XUT emulation for analog trunk, the XDLC emulation module 57 is used to emulate stimulus messages. It communicates with the Telephony Signaling Module 56 to transmit stimulus messages.

[0120] DN-to-IP address translation may be handled by a variety of methods.
Preferably DN-to-IP translation is handled by the gatekeeper 20 using the RAS signaling. Optionally, an Address Translation module 59 may be provided. It collects IP-side information on each client and indexes it by the client's DN. It connects with the management module 52 to accept new configurations and with the network protocol module to perform DN translations. It is present in the leader card 22-4 only. The only manipulation required is to add a leader DN number in front of the internal DN provided by the core switch 24, before sending it to the gatekeeper interface 58.

[0121] The Network Protocol module 53 manages individual calls, receiving and sending SSD, ELAN and H.323 messages according to call status. This module 53 handles the gateway itself, and is present on all ITG cards 22.

[0122] As shown in Fig. 10, the Gatekeeper Interface Module 58 is the interface between the XoIP Line Side gateway 10 and the gatekeeper 20. The H323 standard specifies 4 types of channels: RAS Signaling (registration, admission, status), Call Signaling (CONNECT, RELEASE, FACILITY, ...), Control channel (capabilities exchange, logical channel(s) management, ...) and Logical channel(s) (audio, video, data) The Gatekeeper Interface 58 is responsible for RAS signaling. It is also responsible for forwarding call signaling when the Gatekeeper routed call signaling model is used (for security and management reasons). The tasks done by the Gatekeeper Interface 58 may be:

Gateway (un)registration to the gatekeeper
RAS messages validation (timeout, out of sequence RAS, ...)
RAS interface with other XoIP modules
Interface with IPLL Gatekeeper (DN registration, resource status update, leader card registration and DRQ forward)
No local address translation is required when the routed call signaling model is used. In this case call signaling messages are directly sent to the Gatekeeper 20. To reduce the size of the CPU on the leader card 22-4, the leader card 22-4 need not be required to perform routed call signaling to follower cards 22-5, 22-6. Each follower card 22-5, 22-6 then has to register itself. But following a request from the Gatekeeper 20, the leader card 22-4 may be responsible for allocating a port of a follower card 22-5, 22-6 for incoming calls.

[0123] The gatekeeper interface logical layers are shown in Fig. 11. Being the interface with the gatekeeper 20, the bottom layers are symmetrical to those of the gatekeeper 20 itself Upper layers are providing the interface to each module of the XoIP. The RAS stack is based on the same architecture as the one used by IPLL Gatekeeper. Responsibilities are:

System Layer: This layer provides base OS calls in order to be platform independent. RAS Layer: This is a protocol stack handling H225 RAS messages from the Gatekeeper 20. As for an IPLL Gatekeeper, this stack is provided by RadVision (RV). It provides a mechanism to register callback procedures which are used for incoming RAS messages. RADVision Interface Layer: encapsulates RADVision API for upper layers in order to stay vendor independent.
RAS Handler Interface implements the RAS call back functions.
RAS Protocol State Machine manages timers and error conditions for receiving incorrect or out of sequence RAS messages.
Nortel H323+ Database loader Layer: it implements a Nortel proprietary protocol between the Gateway 10 and the Gatekeeper 20. The Gateway 10 sends to the Gatekeeper 20 the list of valid DN through this interface.
Gatekeeper Manager Interface is responsible for communication set up with the Gatekeeper 20 during ITG boot or shutdown sequence. It implements *discovery, registration* and *unregistration* procedures as described in H323. It also implements *DN upload* mechanism.
Address Gatekeeper resolution: this interface provides the ability to request address resolution from the Gatekeeper 20. This is used when local resolution (address resolution module 59) fails. Gatekeeper resolution requests should normally not be used when call signaling messages are always sent to the Gatekeeper 20.
Resource Manager Interface: this interface is responsible for communications between ITG Resource Manager module 51 and the Gatekeeper 20. It implements mechanisms for *resource creation/destruction, admission* and *status* requests, as well as *disengage* messages.
Network Protocol Interface: This can be split into two: RAS specific messages handling and non-RAS messages handling. It implements mechanism for *bandwidth* changes, *status* and *request in progress* RAS messages.
H323 layers: These layers handle non-RAS messages of the H323 standard.

[0124] Fig. 12 shows Gatekeeper Interface interactions (and only those) with other modules. Module Interface (IF): this is an interface layer specific to communications between a given module and the Gatekeeper Interface 58. This is implemented on each module in order to ease re-usability of the Gatekeeper Interface.

Network Management Module 52: this module can be used to configure the Gatekeeper Interface 58 (like the well known discovery address). Configuration data are sent to the Gatekeeper Manager Interface.
Network Protocol Module 53: this module interacts with the Gatekeeper interface 58 for a call signaling channel which is routed through the Gatekeeper 20. This is also used for bandwidth change, status and RIP RAS messages. Interactions are done through the Network Protocol Interface layer.
Address translation module 59. When such a module is present it implements a local address resolution mechanism in order to speed up call setup. If address resolution fails locally, a request may be made to the gatekeeper 20 through the address resolution interface. The module 59 is optional. Address resolution may be done in the gatekeeper 20.
Diagnostics Module 60: this module is responsible for diagnostics and alarms. It includes alarms specific to the Gatekeeper Interface 58 (RAS reject messages).
System Monitor 61: this module is responsible for starting a discovery and a registration process.
Security Module 62: this module is responsible for Authentication of the Gatekeeper 20 and incoming RAS messages based on tokens.
Resource Management Module 51: this module interacts with the Gatekeeper Interface 58 for resource creation/destruction, status and admission RAS messages. This is done through the Resource Manager Interface layer.

[0125] Messages shown in Figs. 13 to 21 refer to Gateway-Gatekeeper communication (e.g. registration and admission). The Gateway 10 exchanges two types of messages with Gatekeeper 20: H323 standard messages (RAS - Registration Admission Status) and Nortel proprietary messages. The H323 standard messages (RAS) messages correspond to the standard definition and their detailed description, including fields, can be found in the H225 recommendation. ARQ/DRQ messages, even if standard in their definition, have been slightly extended in their use.

[0126] Gatekeeper discovery is the process that the Gateway 10 uses to determine which Gatekeeper 20 to register with. By default it is done manually, the Gatekeeper Interface is configured by the administrator for a gatekeeper and alternate gatekeepers. But if these addresses are not provided and only in that case, the discovery process is automatically started (Fig. 13, GRQ - GatekeeperRequest, GCF - GatekeeperConfirm, GRJ - GatekeeperReject). If it fails (GRJ message), an alarm is sent to the Diagnostics module 60.

[0127] All ITG cards 22 register (Gateway registration messages see Fig. 14, RRQ - RegistrationRequest, RCF - RegistrationConfirm, RRJ - RegistrationReject) to the Gatekeeper 20 after Gateway discovery is completed by the Leader card 22-4. If the registration fails, the Gateway 10 tries alternate gatekeepers 22. If it also fails, an alarm is sent to Diagnostics module 60. An alternative Gatekeeper address can be sent in an RCF message of the primary Gate-

keeper. This address, even if different from the one datafilled, is the one to be used so that the primary Gatekeeper can send the address of a backup/mirror Gatekeeper. Alternate Gatekeeper addresses datafilled are only used when Gateway fails to connect.

[0128] All ITG cards 22 register as gateway for the client terminal type. Leader and Backup Leader cards provide each other with addresses in the 'alternateEndpoints' field. The Gatekeeper is aware of which card is the leader card as it is specified when downloading the DN table.

[0129] Both the Gateway 10 and the Gatekeeper 20 can start the unregistration process (Gateway unregistration messages, see Figs. 15 for gateway-gatekeeper messages and Fig. 16 for gatekeeper-gateway messages, URQ - UnregistrationRequest, URJ - UnregistrationConfirm, URJ - UnregistrationReject). This is done by the gateway 10 when a card 22 is brought down. If the Gateway 10 receives an unregistration reject from Gatekeeper 20 an alarm is sent to Diagnostics module 60. The Leader card 22-4 can send an URQ if the Backup Leader card shall be used. The Gatekeeper 20 can send an URQ to all ITG cards 22 if the alternative Gatekeeper must be used. In this case the ITG cards 22 must send an RRQ to the alternate Gatekeeper.

[0130] The Gateway 10 requests access to the LAN through ARQ message (Gateway to Gatekeeper admission messages ARQ - AdmissionRequest, ACF - AdmissionConfirm, ARJ - AdmissionReject, see Fig. 17). If access is not granted, an alarm is sent to Diagnostics Module 60.

[0131] The Gatekeeper 20 to Gateway 10 ARQ message (Gatekeeper to Gateway admission messages see Fig. 18) is proprietary in its use and allows concentration.

[0132] In accordance with an aspect of the present invention the gateway 10 may request QoS changes from the gatekeeper 20 and vice versa. For example, the gatekeeper 20 or the gateway 10 may request a change in LAN bandwidth allocation (se Fig.

[0133] The Gateway 10 preferably informs the Gatekeeper 20 that a call is being dropped (as the Gatekeeper needs to know about the release of bandwidth- Disengage messages, see Figs 20 and 21, DRQ - Disengage Request, DCF - Disengage Confirm, DRJ - Disengage Reject). The Gatekeeper 20 can also force a call to be dropped. All DRQ messages are preferably forwarded by the Gatekeeper 20 to the Gateway 10 for the Gateway 10 to know that call has ended. This is necessary for billing as 'release complete' might not always be sent.

[0134] Proprietary messages between the Gateway 10 and the Gatekeeper 20 have been implemented for the following reasons:

the Gatekeeper 20 must know the list of DN recognized by the Gateway (10 Gatekeeper requirement).
In order to give the right answer to incoming calls, the Gateway 10 must store the locally status of IP sets.
Leader and Backup Leader cards must tell the Gatekeeper 20 of their use.
In order to achieve concentration and as the Gateway 10 is doing resource management, the Gatekeeper 20 must request from the Gateway 10 a channel for each incoming call.
As a 'release complete' message might not always be sent at the end of call, the Gatekeeper 20 must tell the Gateway 10 when call is ended to perform billing.

Here is a list of proprietary messages:

DN upload
Once the gateway 10 has performed RAS discovery and registration with the 20, the core switch 24 through the leader card 22-4 sends to the Gatekeeper 20 a list of valid DN. This is done on a separate reliable TCP/IP connection. The TCP/IP port to be used is sent to the Leader card 22-4 in the RCF message. Once upload has been completed, the connection is closed, but the port remains available on Gatekeeper 20. Further updates are done incrementally using the same port.
Database download (optional)
Where local address resolution is available (optional Address resolution module 59), a copy of the DN address table is downloaded from the gatekeeper 20. This is done on request from the leader card 22-4 after the gateway 10 has performed RAS discovery and registration with the gatekeeper 20. It is preferably done on a separate reliable TCP/IP connection which is closed when the transfer is complete. Further, updates may be performed through RRQ and URQ messages.
Resource status (resource registration/unregistration)
The Gatekeeper 20 informs the Gateway 10 of resources which have registered, unregistered or which have failed polling. This is done through standard H323 ARQ and URQ messages.
Channel allocation and leader card registration
As the leader card 22-4 can perform channel allocation, the Gatekeeper 20 sends an ARQ to it for incoming calls. The leader 22-4 sends back an ACF with the IP address and port of the follower card 22-5, 22-6 to be used. For this reason, Leader and Backup Leader cards register to the Gatekeeper 20 in a special way. For example, the

Leader and Backup Leader provide each other's address in an RRQ message, the address of the leader card is sent to the Gatekeeper 20 during DN upload.
End of call
The Gateway 10 must be aware of call end in order to perform billing. This is usually seen using 'release complete' message. In some cases, this message is not used and a DRQ is sent. For this reason all DRQ messages sent or received by Gatekeeper 20 are forwarded to Gateway 10.

It is necessary to match a DN to the corresponding IP address for outgoing calls. The present invention includes:

Full internal address resolution

[0135] The address resolution is downloaded from the gatekeeper 20 during start up. The table is dynamically updated by the gatekeeper 20 which forwards registration/unregistration endpoint information to the gateway 10. If a local resolution cannot be achieved, the gatekeeper is sent a resolution request.

Partial internal address resolution

[0136] The gateway 10 stores a table of the most recently used and/or most called addresses. if an address is not matched internally a request is made to the gatekeeper 20.

Full gatekeeper address resolution

[0137] This is a preferred solution and is covered by standard H323.
The operation of the above embodiments will now be described in detail. The H.323 Standard defines four communication channels for call establishment:

H.225 RAS Signaling between End Point/Gateway and Gatekeeper
H.225 Call Signaling (Q.931 messages)
H.245 Call Control (Master/slave determination, Set capacity exchange) media Channel (voice)

[0138] In certain embodiments of the present invention, the Gatekeeper and MMCS Gateway call signaling routed model is preferably used; i.e. all call signaling goes through Gatekeeper 20 and MMCS Gateway 10. However, the present invention is not limited thereto. For example, call control and the media path may be or may be not routed through the gateway 10 for IP client-IP client calls. The present invention includes the following possibilities:

call signaling from and to the client goes to the gateway 10 via the gatekeeper 20 (Fig. 22). RAS signaling goes to the gatekeeper 20 from the client. Call control goes between the client and the gatekeeper.

call signaling and call control go through the gatekeeper 20 to the gateway 10- see Fig. 23.

call signaling and call control go between the client and the gateway 10. RAS signaling goes to the gatekeeper 20 from the client.

As one example, in case of an IP client 16 - SCN 14 call, all H.323 channels can go through the MMCS Gateway 10 (see Fig. 22). The media path and call control are handled between the IP client 16 and the gateway 10 through the IP network 12. The RAS authorization signaling is handled between the client 16 and the gateway 10 and the gatekeeper 20. For a call between IP clients 16, 18 (Figs. 24, 25) call signaling goes via the gateway 10. The RAS authorization signaling is handled between the calling client 16 and the gateway 10 and the gatekeeper 20, whereas call control and the media path is between the clients 16, 18. In this way double compression/decompression per call is prevented. If the called IP client 18 is not served by the same gateway as the calling client 16 (Fig. 25) the media path and call control still pass directly through the IP network without involvement of the GK 20 or the GW 20 and therefore without double encoding/decoding. Call signaling and RAS authorization is carried out between the client 16, 18 and the local gatekeeper 20, 20' or gateway 10, 10', respectively. After authorization and address resolution for the called party the IP address of the called party is forwarded to the calling client 16 so that the call can be set-up through the IP network 12 independently of the GW 10, 10' or the GK 20, 20'. To provide the signaling path between the gateways 10, 10' each gateway 10, 10' is associated with a trunk side functionality 25, 25' for routing the messages through the IP network 12. For example, the gateways 10, 10' may be provided with trunk side IP gateway cards 25, 25' for handling trunked connections between MMCS' 10, 10'.

[0139] In the following the Call Signaling exchange between an SCN set, the MMCS Gateway, the Gatekeeper and one or more IP Clients is described.

Basic Call Overview: IP<->SCN

[0140] An overview of the Call Signaling exchanged between an SCN calling set and an IP Client 16 and between an IP Client 16 and an SCN receiving set for various embodiments of the present invention is shown in Figs. 26 and 27. More detailed flows are shown in Figs. 29-31 The notation of Fig. 28 is used in the message flows of Figs. 29-31.

[0141] With reference to Fig. 26 with a call from an SCN, e.g. a PSTN (set A) the first step is to find a PTN from the pool available. This request is done by the core switch to the gateway (MIX GW). Once a PTN is associated with a virtual TN the IP client profile (e.g. which supplementary services are available and authorized) is dynamically linked to the call. The access is requested from the gatekeeper via ARQ/ACF messages. Finally the call is set up with the IP client (IP terminal B). The call process from the IP client (see Fig. 27 is similar).

[0142] A more detailed flow is shown in Fig. 29 for an outgoing call to an IP network IP client IP B from an SCN set A. The call is first received by the core switch CS (24) which returns a Call Proceeding and an ISDN ALERT message. The SETUP message from the SCN 14 includes the DN of the called party DNb and of the calling party DNa (ISDN connection is assumed). The next step is to retrieve a Physical TN on the ITG card 22. The request for a PTN is done by the core switch CS to the ITG leader card via Ethernet which returns an available physical port of one of its ITG follower cards. While requesting a PTN, the core switch CS is also conveying call processing information (e.g. called party number, calling party name) for which no SSD messages currently exist. Once a PTN is associated to a Virtual TN, the call can go on using SSD signaling between the Core Switch CS and the ITG card. The ITG handles then the call to the IP network thanks to the DSP component 32 (voice compression and packetization) and the host component 34 (fig. 7, XDLC emulation, H.323 protocol interface).

[0143] The next step is to gain admission to the IP network 12. This is done by ARQ/ACF messages to and from the gatekeeper. Once admission is granted, an H225 SETUP message is sent to client B from its follower using the IP address of client B. In response to the H225 SETUP message the IP client B returns an H225 ALERTING message. If the call is accepted an H225 CONNECT message is sent from client B to the follower. The follower communicates with the core switch CS via SSD signaling. The CS then sends an ISDN CONNECT message to the SCN set A and the call set up is completed. The speech path goes between the SCN set A and the follower and the necessary code translations are made, e.g. from the SCN PCM speech to the compressed digital speech on the media path in the IP network 12.

[0144] A call to a busy IP client B does not generate any signaling between the core switch CS and the ITG card 22. Instead the status of the H.323 terminal is continuously stored with the associated VTN on the core switch CS which can directly provide the appropriate treatment (e.g. hunt, busy tone).

Abnormal operation

[0145] When the Called IP Client rejects the H.225 SETUP message (see Fig. 30), an SSD RLS key pressed is sent to the Core Switch CS. If the called party is a traditional set, this SSD is ignored: in fact, on a Core Switch point of view it is not possible for a called Aries set to disconnect the call before it is answered. If the called party is an IP set, the calling party is disconnected

Incoming IP to SCN Call

[0146] An incoming call from an IP client A on the IP network 12 is first seen on the gateway as an ARQ message (Fig. 31). The leader card selects a PTN from the pool (following load sharing criteria), reserves it and informs the gatekeeper to instruct client A to forward the received H225 SETUP onto the associated follower card thanks to the callSignalAddress information included in ACF message. When the follower receives the H225 SETUP, it retrieves the PTN which was reserved and generates an incoming call using SSD signaling on that PTN. The core switch then handles call termination with the SCN using ISDN signaling.

Basic Call Overview: IP<->IP call

IP to IP call managed by the same MMCS Gateway

[0147] When both calling and called IP Clients A, B (Fig. 32) are managed by the same MMCS Gateway, separate PTN's must be allocated to each client from the pool of available PTN's. Further, each client must be authorized by the Gatekeeper. As described previously for a call from an IP client the MMCS gateway first receives an ARQ from the

calling party at the leader. The leader selects a PTN for both clients (PTNa and PTNb) from the available pool and stores them. The A follower informs the gatekeeper with an ACF to forward the H225 SETUP message from the client A to the A follower. The IP address of a follower (Fa) is returned to the client A in the ACF message. The client A sends an H225 SETUP message back to the A follower. When the A follower receives the SETUP message it retrieves PTNa and generates an incoming call (IC call) through the core switch CS using SSD signaling. The core switch CS initiates an outgoing call (OG call) via the B follower which retrieves the stored PTNb and obtains admission to the network from the gatekeeper with ARQ/ACF messages. The B follower then sets up a call to the IP client B using the procedure previously described. The following information has to be propagated between the respective Followers cards of the two clients:

The User to User IE (UUIE) which conveys specific IP parameters has to be propagated for the incoming IP->CS call part to the outgoing CS->IP call part.
The IP Follower (F_A) Address used for incoming IP->CS call part is also sent to the Follower Card (F_B) which handles the outgoing CS->IP call part. The Follower Card (F_B) informs also via ELAN the Follower Card (F_A) with its IP Address. So the Follower Cards can communicate together without conveying the data to the Core Switch. This direct communication is used to:

1) convey the H.225.0 ALERT message from called to calling IP Client and,
2) convey some specific supplementary services information as detailed later. To reduce traffic on the ELAN, when the resource manager of the Leader is requested to find an available Follower card (F_B) for the outgoing CS -> IP part of the call, the resource manager chooses if possible the same Follower card as Follower card (F_A) used for the incoming IP->CS call part.

[0148] Fig. 33 details the IP to IP call termination. As H.225 may be closed during call termination procedures, the H.225 RELEASE COMPLETE message may not be sent by the IP client. In any case, H.225 RELEASE COMPLETE and Disengage Request (DRQ) RAS messages are a trigger for the ITG card to disconnect the call and to inform the Core Switch.

IP to IP call managed by a different MMCS Gateway

[0149] When calling and called IP Clients are managed by different MMCS Gateways (see Fig. 34) the call is seen as two IP <->SCN calls back-to-back with a trunk call between the two gateways: the Trunk part of the IP call between the two MMCS Gateways is seen by MMCS Core Switch as an SCN trunk call, so a detailed description is not necessary. The message flows (Figs. 29, 31) between core switch and SCN and vice versa are applicable with the addition of a trunk call between the two MMCS gateways. To achieve this it is necessary to communicate some information from the first gateway MMCS gateway 1 to MMCS gateway 2. For instance, the UUIE has to be propagated from calling IP Client to MMCS Gateway 1, from MMCS Gateway 1 to MMCS Gateway 2 and from MMCS Gateway 2 to called IP Client.

Non-call related operation

[0150] Specific operations are required in order to (re-)synchronize non-call related data between MMCS Core Switch, Leader/Backup-Leader cards and Gatekeeper. Several events may cause this (re-)synchronization:

- MMCS System (i.e. Core Switch and ITG cards) start-up
- Core Switch System load
- Gatekeeper, Alternative Gatekeeper switchover
- Leader, Backup Leader switchover

The following information needs to be updated:

- Gatekeeper IP address in the ITG Cards
- Core Switch configured IPSET DNs in the Gatekeeper
- Gatekeeper DN Status in the Core Switch
- Leader IP address in the other ITG cards, in the Gatekeeper and in the Core Switch

Gatekeeper IP address notification to MMCS gateway

DN table

Purpose of the DN table

[0151] The DN table is a list of valid DNs (i.e. DNs of IPSETs declared in the core switch). This information is required by the gatekeeper to allow IP client registration. As IP clients register themselves using E.164 numbers, the gateway converts DNs into E. 164 before sending them to the Gatekeeper. This way, when an IP client registers to the gatekeeper, the gatekeeper is able to check if this IP client is known by the gateway. The DN table is built and sent to Gatekeeper either following IPSET service change or after core switch system load or at Gatekeeper request. Address of the leader card is also sent during full DN table download.

Message flow

[0152] DN entries are maintained by the core switch. They are propagated to the Leader Card and the Gatekeeper. The Gatekeeper can then allow registration of endpoints with corresponding DN.
Data can be sent in two ways: fully or incrementally. The process can be initiated by any party at any time. A TCP/IP connection is used for all transactions. The TCP port to use is sent by the Gatekeeper in RCF message and remains available until unregistration.
[0153] **Incremental update** The Core Switch sends to the Leader Card an incremental update of a DN entry in one of the following case: New DN or Delete DN.
Remarks:

A DN change is seen by the leader card as a DN delete and new.
More than one DN can be added or removed in one message.
Leader card forwards changes to the Gatekeeper.
When the full DN table is loaded to the Gatekeeper, registration status is set to unregistered.

[0154] **Full DN upload:** The Core Switch sends to the Leader Card all DN entries in one of the following case:

Core Switch System load
Request from Leader card (after a request from GK).
Each DNTableDownload message contains N DNs (where N is to be defined depending on the number of VTNs that can be scanned during a timeslice). Each packet might contain redundant data. Data exchange is made through TCP/IP. The Leader Card reconstructs the whole table in memory before forwarding it to the GK with its own address (so that Gatekeeper knows which card is responsible of resource management).

Remark: 'DNTableUploadRequest' message is sent through UDP and contains the TCP port to be used for the DN table download.

Impact on Core Switch

[0155] Each time a service change is performed on an IPSET concerning the DN, a message is sent to the leader and then to the gatekeeper in order to update the DN table. The following rules apply to the messages sending:

- for REQ=NEW, no check is performed on the DN sent in the message for the case it has already been defined for another VTN and thus, already been sent to the gatekeeper.
- for REQ=CHG, only the "Add" message is sent if the old DN still exists for one or more VTN(s).
- for REQ=OUT, no messages are sent if the removed DN still exists for one or more VTN(s).

In the same manner, when the entire DN table is downloaded to the gatekeeper, there is no check performed by the core switch in order to remove DNs which exist for several VTNs. In every cases, the leader card is responsible for removing redundant DNs.

Impact on leader

[0156] The leader is responsible for removing the redundant DNs sent by the core switch.

Impact on gatekeeper

[0157] The Gatekeeper maintains a table with E. 164 numbers with their registration status.

DN registration

[0158] When an IP Client gets registered or unregistered by Gatekeeper through RRQ/RCF or URQ/UCF RAS signaling, the Gatekeeper informs the MMCS Core Switch of this registration status. This is done by:

- standard RRQ and URQ messages between Gatekeeper and Leader card,
- DNRegistrationStatus messages between Leader card and Core Switch

[0159] At reception of a DN Registration Status message, the Core Switch updates the *Registration* flag of all the IPSETs (i.e. all the VTNs) which have the same DNa.

Abnormal Feature Operation

[0160] This section covers cases of abnormal operation e.g. database inconsistencies between the ITG leader DN database and the core switch DN tree, as well as some cases involving core switch restart or initialize. One of the main facts to consider, is that, in the case of a call to the IP network, the state machine of the MMCS software has reached the "ringing" state before the ITG has had a chance to start on the protocol. This means that, in most cases of abnormal termination, the call is given the 'no answer' treatment by the core switch. In all cases, the elimination of single points of failure is the priority.

Simple call abnormal operation

[0161] The simple call abnormal operation includes dialing an invalid DN from an IP client, trying to reach an IP client that is not registered with the system, insufficient resources on the core switch, or an IP client through a congested network. In case a call from an IP client is denied a H.225 RELEASE COMPLETE message is sent to the IP client instead, with a RelComp Reason code appropriate to the situation.

[0162] The fact that an IP client dialed an invalid DN is determined at the core switch. H.225 requires sending a RELEASE COMPLETE message to the IP client, with invalidRevision in the ReleaseCompleteReason field

[0163] The gatekeeper keeps track of IP clients present on the network, and informs the ITG leader of their presence in real-time. This information is not extended to the core switch, and a call to an absent IP client is given the no-answer treatment by the core switch.

[0164] If the system lacks resources to establish a call (such as ITG ports, tone units, or available talkslots), the call is denied even though the resources may not be needed per se (talkslots for IP-to-IP calls). When such a condition occurs on the core switch, the call is taken down. In case of an IP originator, the RelComp Reason is gatekeeperResources or noBandwidth.

[0165] If the call is rejected by the far end of an IP-to-PSTN call, the ReleaseCompleteReason is mapped to the corresponding Cause IE code as specified in section 8.2.2.8 of the H.225 document.

[0166] If the ITG leader can be made aware of degraded QoS to a given IP client, no call attempt is made on the IP network to that IP client. In this case, signaling is returned to the core switch to mark the call as ringing until the no-answer processing triggers.

[0167] Incoming calls from IP clients in a congested situation are assumed to be dealt with by the gatekeeper.

[0168] When a call coming in from the IP network attempts to use a resource that was just removed or disabled by a maintenance or service change operation the offending call will be denied by the core switch software. The case of calls from the PSTN is handled by the core switch software.

Supplementary Services

Call Transfer

Definition

[0169] In all the following sections, a call (called primary call) is established between User A and User B. User A (called Transferring Party) transfers User B (called Transferred Party) to User C (called Transferred-to Party). User A, B and C can be SCN sets or IP clients.

Call Transfer is implemented on a mixed SCN/IP network as detailed in Fig. 35.

Call Transfer methods

[0170] On an IP Network, the H.450.2 Standard defines call transfer with the rerouting methods (with or without consultation). On an SCN Network, MMCS Core Switch only implements call transfer by joining the primary and secondary calls (call A-B and A-C). Call transfer is handled either by the MMCS Core Switch or by the Transferred-to IP clients depending on the Users set type (i.e., SCN sets or IP clients) as detailed below

Gatekeeper Interaction

[0171] The Gatekeeper routed model is preferably used for an H.323 basic call. As the Gatekeeper supports only H.323 basic call, call transfer operations are transparent for the Gatekeeper.

Notations

[0172] The notations of Fig. 36 are used in the message flows of Figs. 37 to 44

Call transfer operations

[0173] When the transferring party is a SCN set, call transfer by joining the two calls is handled by the MMCS Core Switch whether User B and C are SCN sets or IP clients.
Notes:

No call transfer indication (ctComplete or ctUpdate invoke) is provided to the IP Transferred or Transferred-to Clients.
As the Transferring SCN set is not a set managed by the MMCS Core Switch (MMCS supports only IP sets), the MMCS Core Switch is not available to prevent a double compression/decompression if the Transferred and the Transferred-to Parties are IP Clients.

When the transferring party is an IP Client, specific methods are required in this case and is explained below.

Transferring and Transferred Parties are IP Clients, Transferred-to Party is an SCN Set

[0174] As shown in Fig. 37 call transfer by rerouting is handled by the Transferred IP Client.
When IP Client A transfers the primary call, a ctInitiate invoke is sent to Follower card (F_A). If this primary call is an IP to IP call, the APDU is conveyed by the Follower card F_A via ELAN to the Core Switch (Note that Follower card F_A was informed during call establishment ifB is an IP Client or a SCN set). The Core Switch checks if Client A can transfer the primary call. In this case, the received information is sent via ELAN to the Follower card (F_{B1}) which handles the IP call to B. The Follower card F_{B1} rebuilds the ctInitiate invoke and sends it to B.
[0175] At reception of this message, the transferred Client B initiates a new call which is handles by Core Switch like a basic call. The Core Switch uses another VTN available for this IP Client B for this secondary call.
Note: if transfer is not allowed from A, Core Switch sends a reject to Follower card F_A which builds a ctInitiate return error and sends it to Transferring Party A.

Transferring Party is an IP Client, Transferred and Transferred-to Parties are SCN Sets

[0176] If the Transferring Party A is an IP Client (see Fig. 38), and Transferred B and Transferred-to C Parties are SCN Sets, the call by join method is used to transfer B to C. Call transfer is handled by MMCS Core Switch. As Follower card F_A knows that B is an SCN set, at reception of a ctInitiate invoke, Follower card F_A sends SSDs messages to initiate call transfer on MMCS Core Switch. At reception of an ALERT message from the Transferred-to party C, Core Switch sends via ELAN a RequestForXferComplete message in order that Follower card F_A sends the SSDs messages to complete the transfer.
Notes:

the TRN key is hard-coded for the IPSET in the Core Switch and in the ITG cards.
The Transferred-to party C can an IP Client or a SCN Set.

Transferring, Transferred and Transferred-to Parties are IP Clients

[0177] If Transferring, Transferred and Transferred-to Parties are IP Clients (see Fig. 39), call transfer by rerouting is handled by the Transferred IP Client. The H.225.0 ALERT message which contains the ctSetup.rr APDU is directly conveyed from the Transferred-to Follower to the Transferred Follower Card..

Transfer with consultation

[0178] When a secondary call is already established between IP Client A and the Transferred-to Party C, A transfers B to C using the "Transfer with Consultation" method: a ctIdentify invoke is sent from A to C in order to know if C can participate in the call transfer.

[0179] <u>If Transferring and Transferred-to Parties A and C are IP Clients</u> (see Fig. 40), the ctIdentify invoke (respectively ctIdentify response) is transparently conveyed to C (respectively to A) via the Follower cards F_A and F_C. (Note that Follower cards F_A and F_C was informed during call establishment that they handle the same IP to IP call).

[0180] <u>If Transferrin Party A is an IP Client and Transferred-to Party C is a SCN set</u> (see Fig. 41), at reception of the ctIdentify invoke, the Follower cards F_A sends back a ctIdentify response to the Transferring IP Client A with DNc as rerouting Number.

Call Forward

[0181] H.450.3 Call Diversion messages are used only for Call Forward All Calls feature activation. No H.450. 3 messages are used for call processing. All call diversion processing is done in the Core Switch.

Call Forward All Calls/Call Forward Unconditional

Call Forward Activation/Deactivation

[0182] These following sections describes the Call Forward feature Activation/Deactivation from an IP Client. Call Forward feature can be activated if the Radvision H.323 stack supports H.450.3 *activateDiversion* and *checkRestriction* operations and if the IP Clients provide this information.

<u>**Local activation**</u>

[0183] An IP Client A activates CFAC by sending to the diverted-to party a H.225.0 SETUP message with the H. 450.3 *checkRestriction invoke* operation (see Fig. 42). As call signaling is routed to the MMCS gateway, the MMCS gateway:

- intercepts this message,
- activates CFAC to the diverted-to party in the MMCS Core Switch and
- sends back to IP Client A a H.225.0 CONNECT message with the H.450.3

checkRestriction returnResult (respectively *checkRestriction errors*) operation if CFAC is activated (respectively is not be activated) on the MMCS Core Switch.

<u>**Remote activation**</u>

[0184] An IP Client A activates remote call forward of B (served party) to C (diverted-to party) by sending to the served party a H.2250 SETUP message with the H.450.3 *activateDiversion invoke* operation (see Fig. 43). This SETUP message is transparently conveyed by the MMCS GW to the served party. Then the same message flow occurs as for the local activation.

<u>Notes</u>: the H450.3 protocol allows activation of CFU, CFB or CFNR by this way. But on the MMCS Core Switch only CFU can be activated by an User party. CFB and CFNR is configured by the Administrator. Therefore H.450.3 operations with other profile than CFU are rejected by the MMCS Gateway.
Note that B must be an IP Client and has to be is the same IP zone than IP Client A. C can be an IP Client in the same or a different IP zone or can be a traditional set.

[0185] Fig. 44 details the corresponding MMCS Gateway internal message flow: the activateDiversion invoke is

conveyed in the UUIE like other basic call IP parameters. Note that the CFW key is hard-coded for the IPSET in the Core Switch and in the ITG cards.

Call Forward feature operation

[0186] Call Forward All Calls (CFW) allows all incoming calls to a terminal to be automatically forwarded to a pre-selected destination, within or outside of the switch. Call Forward All Calls is supported on IP Clients.

Call Forward No Answer

[0187] Call Forward No Answer (CFNA) automatically forwards an unanswered call to another DN after a customer specified number of rings. The class of service Call Forward No answer Allowed (FNA) activates the feature on a TN basis. Customer options can be defined for DID, non-DID and local calls to deny CFNA for all stations, to CFNA to an assigned hunt DN or a flexible CFNA DN defined per TN.

[0188] Calls terminating to a IP Client not answered within a given time frame can be subjected to CFNA redirection. In addition, a IP Client which initiates a call to a set or terminal can be subject to CFNA redirection. Furthermore, a IP Client DN can be defined as a CFNA DN.

Call Forward Not Registered

[0189] Call Forward Not Registered is handled by the Nortel proprietary Hunting feature: When an IP Client is not registered in the Core Switch, the call is <u>immediately</u> forwarded to HUNT DN if configured, otherwise intercept treatment is provided.

Hunting

[0190] Hunting allows calls which encounter busy DNs to be automatically routed to another DN. Hunting continues along a hunt chain until an idle DN is found, the end of the hunt chain is reached, or the maximum number of hunt steps is exhausted. Short Hunt hunts along the DN keys defined on a station.
The following three types of hunt chains are supported for calls terminating to IP Clients

- Circular hunting
- Linear hunting
- Secretarial hunting

Short hunting is not applicable to IP Client, which supports only a single directory number.
[0191] For calls originated from IP Clients, all four types of hunting can be applied.

IP Clients - Virtual TNs Configuration

[0192] In order to create IP clients through use of VTNs, phantom loop(s) must firstly be created and VTNs are taken from that phantom loop. Up to 1024 VTNs can be configured on a single phantom loop. Once the phantom loop has been created, IP clients (VTNs) can be configured on it through MAT. MAT is a PC based tool which craftspersons use to perform terminal administration through a graphical user interface. The program then converts the input into a script and "drives" the terminal administration overlays by loading the correct overlay and automatically entering the desired response for each prompt.

RADIUS client operation

[0193] Implementation of a RADIUS (Remote Authentification Dial In User Service) client on all ITG cards allows per-call information to be sent to an external machine for billing purposes. Only the accounting part of the protocol is implemented.

- ITG card sends a Start record when a call starts.
- ITG card sends an End record when the call is released.
- The End record contains QoS and amount of data sent.
- Both records contain the Called and Calling Party numbers, and the call ID, for call identification and ulterior correlation with CDR records generated by the core switch.

- The RADIUS records are sent out on the maintenance interface, to maximize security.

No correlation is made between the RADIUS record and the corresponding CDR records from the core switch. This part is left to the external billing machine. Note that there can be a difference between call duration found in the CDR and RADIUS records, due to the time elapsed between the moment the call is marked answered on the core switch and on the ITG card.

Configuration

[0194] The MAT interface provides a UI for the configuration of:

- Enable/disable of RADIUS record generation.
- IP address ofthe external billing machine.
- IP port number ofthe external billing machine (default is 1813).
- Key number for check summing RADIUS record data (the desired security is still TBD).

This data is configured at the Node level and is distributed to all of the ITG cards associated with the Node.

Messaging

[0195] The RADIUS client sends two records to the network listener: one at the start of the call and one at the end. The messages are sent by the Follower card actually processing the voice call (i.e. not the DCHIP or Leader if they aren't handling the voice data). The RADIUS protocol uses UDP for message exchange. The client sends a message to the listener and waits for an acknowledgment. If no acknowledgment is received, the client retransmits the record, using the standard exponential backoff scheme. The data is stored on the card until an acknowledgment is received at which time it is discarded. The client will store a maximum of 100 records, which allows for 2 start and 2 end records for each of the 24 ports.

Start Record

[0196] The Start record is sent when the call is answered. It contains the following fields:

a) Calling party number,
b) Originating IP address and port (the port used for the RTP channel),
c) Called party number,
d) Destination IP address and port (the port used for the RTP channel),
e) Call ID,
f) Call start time,
g) Call setup duration (time from call initiation to call answer),
h) Codec used.

Snapshot of remote Gateway's QoS at time of call connect.

End Record

[0197] The End record is sent when the call is released, rejected, or abandoned. It contains the following fields:

a) Calling party number,
b) Originating IP address and port,
c) Called party number,
d) Destination IP address and port,
e) Call ID,
f) Call start time: the precision on this measurement is TBD, but the higher the precision, the more likely the discrepancies between it and the corresponding duration in the CDR record produced by the core switch,
g) Call duration (time from call answer to call release),
h) Codec used,
i) Number of bytes received,
j) Number of bytes sent,

k) Number of packets received,
l) Number of packets sent,
m) Snapshot of latency seen at the end of the call,
n) Packet loss,
o) Snapshot of the QoS at time of call release.

Access Restrictions

[0198] Access restrictions are used to limit individual users' access to the exchange network, private network, services and features. These restrictions can control calls made or answered from certain telephones. The MMCS Core Switch performs access checks based on:

- the Class of Service (COS) of the individual station
- the Trunk Group Access Restriction (TGAR) code of the station
- the area and exchange codes dialed by stations with Toll-Denied COS

If any restrictions are detected when a call is placed, the call is denied and intercept treatment is applied as defined in the Customer Data Block.
For IP Clients, the three access checks can be configured, and the intercept treatment is given if a IP call is denied.
No development effort is required to support Access Restrictions on IP Clients

Calling Line Identification (CLID)

[0199] Calling Line Identification is provided to called IP Clients.

Calling Line Identification Presentation/Restriction (CLIP/CLIR)

[0200] The Calling Line Identification Presentation/Restriction of an IP Client is configured on set basis with Class Of Service (CLS) DDGA/DDGD. As the H.225.0 standard does not support the presentation indicator in the Calling Party Number Information Element, the presentation of the calling party number (of either an IP Client or a traditional Set) can not be conveyed to the called Party if it is an IP Client. As the Calling Party Number is optional, this IE is not included in the H.225.0 SETUP message if the CLID is restricted.

Connected Number / Presentation / Restriction (COLP/COLR)

[0201] As H.225.0 standard does not support the Connected Party Number Information Element in the H.225.0 CONNECT Message, the connected number is not provided to/from an IP Client. Note that with the future H.323+ evolution, COLP/COLR will be supported.
However in case of ISDN SCN call to IP client, Core Switch builds and sends the connected IE in the ISDN CONNECT if necessary.

Calling/Connected Name

[0202] The H.225.0 standard does not define any particular IE to convey the Calling/Connected Name.
The Calling/Connected Name is provided by the MMCS Gateway to an IP Client in the H.225.0 Display Information Element. If the Calling (respectively the Connected) party is an IP Client, the Calling (respectively the Connected) Name is built according to the IP Client name configured in the MMCS Core Switch whatever the name sent by this Calling (respectively this Connected) terminal.

Calling/Connected Name Presentation/Restriction (S)

[0203] Calling/Connected Name Presentation indicator can also be conveyed in the H.225.0 Display Information Element. Class of Service NAMA/NAMD is used to allow or restrict the IP Client name presentation.

Remote Call Forward

[0204] Remote Call Forward is a Nortel feature which facilitates the programming of Call Forward All Calls from a remote station through the use of Flexible Feature Code (FFC).

Call Forward Busy

[0205] Call Forward Busy (CFB) is a Nortel feature which allows a DID call encountering a busy DN to be forwarded to the attendant if the busy station is call Forward Busy Allowed (FBA).

Internal Call Forward

[0206] Internal Call Forward (ICF) allows a user to selectively forward only internal calls to the Internal CFW DN. This feature is activated /deactivated on a per telephone basis using the ICF key and the SPRE/FFCs from SL-1/digital telephones and 500/2500 type telephones, respectively.

ICF is not supported on IP Clients.
But, an IP Client DN can be programmed as an ICF DN.

H.323 Call Waiting

[0207] IP Call Waiting allows alerting a user that another call is being requested while already on the call. By configuring several VTNs (i.e. several DNs) on the same IP Client (i.e. on the same IP address), the MMCS Gateway can present several calls on the same IP Client.

MADN

[0208] IPSET use Multi Appearance DN (MADN) feature with the following limitations:

- MCN key is not supported
- all the sets which have the same MADN are IPSET (VTN) and all these IPSETs represent the same IP Client
- the call to a MADN is presented to only one idle VTN

Message Waiting Indication

[0209] Message Waiting Indication (MWI) allows notifying a set that a local or remote Message Center or Meridian Mail holds a message for it. This indication appears on the set either via a lamp or a key/ lamp pair or via a tone heard when the set goes onhook. As the ITG line Line Side gateway does not offer the capability of exchanging proprietary non call related messages, the core switch is not able to notify the IP client that a message is waiting for it. The MWI information is only known by the core switch and by the Meridian Mail.

3 Way Calling

[0210] 3 Way Calling (i.e. three party conference) is a low priority requirement. It is not supported as it is not planned to implement the H.323 Multipoint Control Units.

End To End Signaling

[0211] End To End Signaling (EES) enables a set to send tones through an established connection.
For IP client to IP client calls, as the media path is direct between the endpoints, EES, if it is supported by the IP clients, is transparent to the core switch. For IP client to PSTN call (including calls to Meridian Mail), EES, if it is implemented on the IP client, is fully supported. The only restriction concerns the way the tone transmission can be affected by packet loss.
[0212] While the invention has been shown and described with reference to preferred embodiments, it will be understood by those skilled in the art that various changes or modifications in form and detail may be made without departing from the scope and spirit of this invention.

Appendix 1

IP TELEPHONY GATEWAY

Reference Diagram Definitions

PSTN environment

- P1: A VoIP subscriber accessing the VoIP network. This is a 2-stage dial (similar to VNET access). Most likely a 1-800 type number.
- P2: A non-subscriber calling, a VoIP subscriber. The number dialed is the subscriber's existing corporate E.164 number. Called number is assumed to be local to P2. If not, then P2's call will be routed through the PSTN LD route.
- P3: Not Supported. Residential customer using an alternate LD carrier
- P4: Customer calling a local number (e.g. a flower shop), and call gets routed over the VoIP network to a call center which may be located in a different geographic location.
- P5: A non-subscriber receiving a call from a subscriber.

"Flowers" Call Center

- User calls a local number and call gets routed to this Call Center
- ACD functionality from Gateway 2 ?

Corporate Environment.

- PBX1 and PBX2 are existing corporate PBX, where employees are homed off (e.g. Nortel's Crystal Bay Meridian 1 PBX)
- Corporate LAN/WAN is an existing corporate LAN (e.g. Nortel's Corwan)
- NOTE: There are no connections between the LAN/WAN and the PBX
- PC5: Not Supported. A PC client running an H.323 client trying to make or receive calls to/from the VoIP (extranet) network.
- GK4: Not Supported. A local corporate gatekeeper trying to access resources from the VoIP (extranet) network.
- PC6: Not Supported. A work at home or roamer coming through corporate dial-up facilities trying to make or receive calls from the VoIP (extranet) network.

Extranet Zone 1.

- Gatekeeper 1: Local gatekeeper managing Zone 1 which includes gateway 1 and PC1 and PC2
- Gateway 1: MMCS node containing several IP trunk and IP line gateway cards
- PC1: transient subscriber accessing VoIP network using a H.323 client running on a PC. PC accesses network through VPDN service through a RAS. PC1 is homed off Gateway1 and registers with Gatekeeper 1.
- PC2: transient subscriber accessing VoIP network using a H.323 client running on a PC. PC accesses network through VPDN service through a RAS. User has a USB phone attached to the PC. PC2 is homed off Gateway1 and registers with Gatekeeper 1. PC2 is also tunneled back to the corporate LAN/WAN for data and email access.

Extranet Zone 2:

- Gatekeeper 2: Local gatekeeper managing Zone 2 which includes gateway 2 and PC3.
- Gateway 2: MMCS node containing several IP trunk and IP line gateway cards
- PC3: transient subscriber accessing VoIP network using a H.323 client running on a PC. PC accesses network through VPDN service through a RAS. PC3 is homed off Gateway2 and registers with Gatekeeper 2.
- PC4: Not Supported. Non-subscriber PC.

Billing Server:

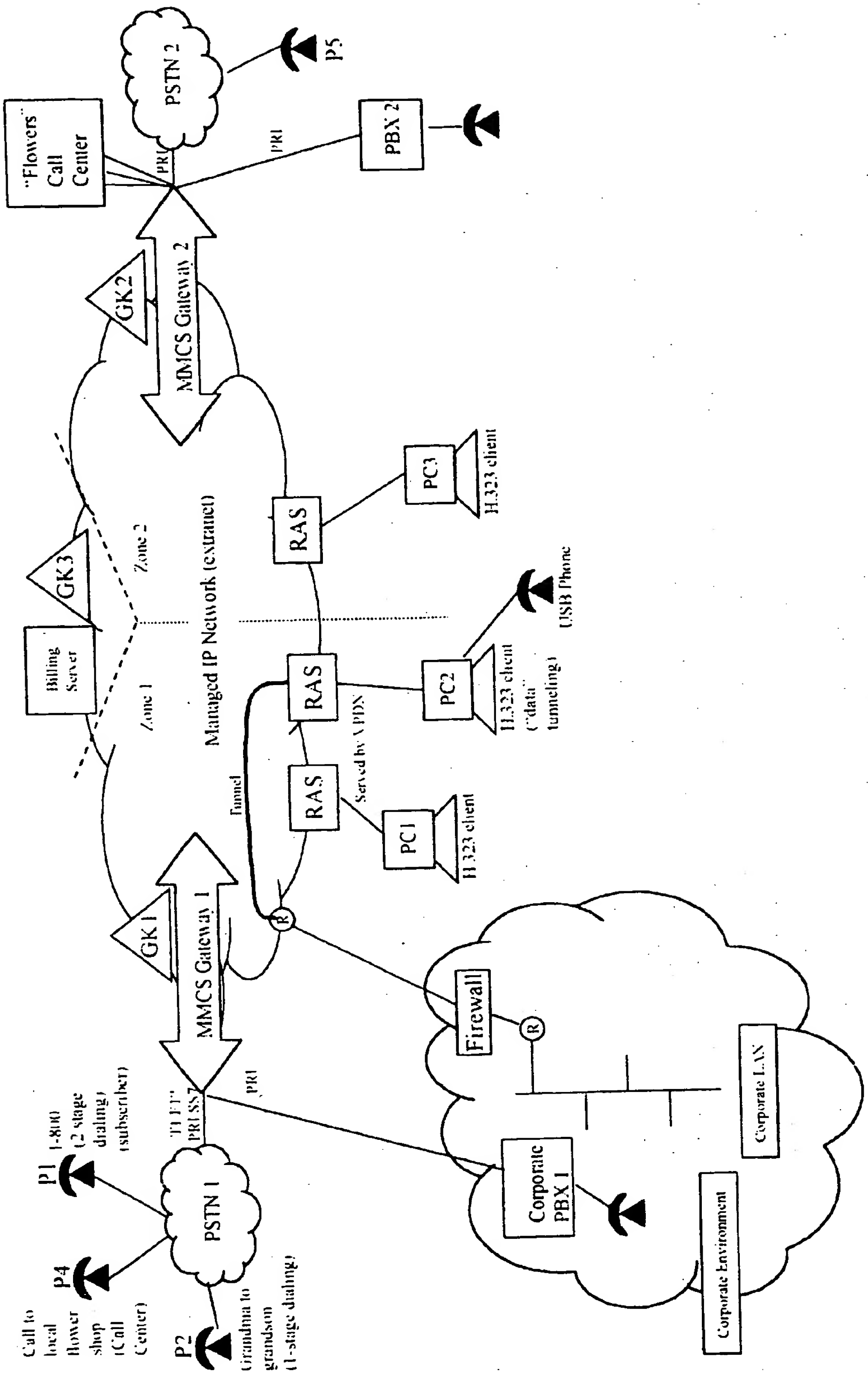
- Aggregates billing records from Gateways and Gatekeepers from all zones.

Gatekeeper 3

- Network Gatekeeper performs local gatekeeper address resolution (i.e. returns Local Gatekeeper IP address given a E.164 number of an endpoint).

Corporate Managed IP Network (extranet) Offer

(reference diagram without unsupported entities)



Assumptions and Key Decisions

- **Voice Quality**, Voice Quality, Voice Quality, priority number 1, then features, priority number 1.0001.
- **One corporate E.164 number**: VoIP subscriber will be reached using his/her existing corporate E.164 number.
  No requirement for a new published VoIP E.164 number - however, an **new** (permanent or temporary) **E.164 IP number** is required for internal use for call forwarding feature or routing within the extranet.
- Gateways and Gatekeepers will be H.323 Version 2 compliant
- No treatment on termination end for CALL HOLD activation on originating end
- CALL FORWARD UNCONDITIONAL (CF-U) sequence must be implemented in gateway card
  Call forward features can be also implemented on the Gatekeeper or the
- Architecture of VoIP must not force user to a different Voice Mail server than the one currently subscribed to
- Multiple Appearance DN (MADN) must belong to same gateway
  Unless the MADN feature is implemented on the Gatekeeper.
- Gatekeeper discovery will be done manually (I.E. provisioned at endpoints)
- Gateway always registers with Gatekeeper
- Gateway will have DID capabilities
- Any calls coming in through Gateway to IP Network, Gatekeeper determines where you are
- Alias Addresses: By default, the user's existing corporate E.164 address will be returned by the Gatekeeper, unless user is registered and has provided a new IP E.164 address. The corporate E.164 address will also be returned as part of the alias address.
- Signaling and Media path routed through gateway for IP calls (to be re-validated!!).
  This assumptions has changed, signalling will still be routed via the Gateways (for the short-term) but the media path is direct to overcome the transit delays through the network

- **No vocodec bypass** in first release (to be re-validated!!!)

Assumptions and Key Decisions (Cont'd)

- **Gatekeeper assumptions**:
  - For first release of Gatekeeper:
    - Keep it simple
    - Direct Mode for Call Control Signalling unless Routed becomes necessary
    - Gatekeeper will NOT perform Gateway resource management (I.e. port allocations, etc..). Push resource management to the edges
    - Push billing to the edges
  - Local Gatekeeper and Network Gatekeeper
    - Local Gatekeeper
      - responsible for intra-zone terminal address resolution
      - handles feature set of terminals
    - Network Gatekeeper
      - responsible for Local Gatekeeper address resolution (may be hierarchical architecture)
      - handles feature set of network

Terminology

Gateway: Refers to MMCS node which includes several gateway cards (line and trunk)

Gateway Line card (alias: IP line): Meridian 1 VPS cards with gateway functionality. IP ports on one side (H.323 compliant) and XDLC terminal emulation (Meridian 1 Line compliant) on the other

Gateway trunk card (alias: IP trunk): Meridian 1 VPS cards with gateway functionality. IP ports (H.323 compliant) on one side and PRI trunk(?) on the other

Gateway to Gateway implies trunk communications

Terminal (IP Client) to Gateway implies line communications

Gatekeeper Procedures

Required zone Management Procedures

Address Translation	Translation of alias address to transport address using a table that is updated with Registration messages. Other methods of updating the tables are also allowed.
Admissions Control	Authorization of LAN access using Admission Request. Confirm and Reject (ARQ. ACF and ARJ) messages. LAN access may be based on call authorization. bandwidth. or some other criteria. Admissions Control may also be a null function which admits all requests.
Bandwidth Control	Support for Bandwidth request. Confirm and Reject (BRQ./BCF/BRJ) messages. This may be based on bandwidth management. Bandwidth Control may also be a null function which accepts all request for bandwidth changes.

Optional Gatekeeper Procedures

Call Control Signaling

There are two models for call control signaling: Direct Mode and Routed Mode. In both modes. when the gatekeeper performs address translation. the gatekeeper provides endpoints with the transport address of the call destination.

In the direct mode. the gatekeeper provides the endpoints with the address of the destination endpoint and directs the endpoints to connect the Call Signaling Channel directly to one another so that all messages can be exchanged directly between the two endpoints without the involvement of the gatekeeper.

In the routed mode. the gatekeeper provides its own address as the destination address so that it receives all call signaling messages and handles routing the call signals between itself and all endpoints during a session. This gatekeeper routed model enables the delivery of supplementary services.

Gatekeeper Policies and Services

Optional Gatekeeper Policies and Services

Call Authorization/Access	The gatekeeper may reject calls from a terminal due to authorization failure. The reasons for rejection may include, but are not limited to, "restricted access to/from particular terminals or gateways", and "restricted access during certain periods of time."
Bandwidth Management	The gatekeeper can control and limit the number of H.323 terminals allowed to simultaneously use the network. Through H.225.0 signaling, the gatekeeper may reject calls from a terminal due to bandwidth limitations. This may occur if the gatekeeper determines that there is not sufficient bandwidth available on the network to support the call. This function can also operate during an active call when a terminal user requests additional bandwidth.
Call Management Services	The gatekeeper may maintain a list of ongoing H.323 calls that is similar to PBX logs. This information may be necessary to indicate that a called terminal is busy, and to provide information for the Bandwidth Management function.
Supplementary Services	Supplementary Services, such as call FORWARD and TRANSFER are critical telephony functions users will expect their network to provide. H.450 provides a mechanism for implementing supplementary services.

Nortel Differentiators

Supplementary Services

- Call forward: Call forward on busy, Call forward no answer, Call forward unconditional,Call forward not registered
- Voice Mail for Call forward conditions
- Call hold
- Call transfer
- CLID
- CLID Restriction
- Calling Name
- Multiple Ringing on DNs (MADN): inbound call will ring on 2 different extensions at the same time
- Multiple Line Appearance: a single phone is the destination of multiple E.164 numbers
- 3-way Calling or conferencing (Max. 1 IP device)

Refer to APPENDIX B for Supplementary services invoked from a IP terminal.

Procedures and Policies

- Authentication of endpoint: You are who you say you are
- Call Routing: Ability to route call to different destinations.
- Billing Support
- Credit Card / Prepaid card
- Dialing Plan: North American, International

Gatekeeper/Gateway functionality Breakdown

Functionality	Gateway/MMCS	Local Gatekeeper/MMCS	Network Gatekeeper
Address Translation	N/A	Maintains mapping of local E.164 nnx address to the transport address (IP+port) of the IP terminal. Translates called E.164 to a transport address (IP+port) of Gateway if in same zone. If not, the Network Gatekeeper is queried.	Maintains mapping of the E.164 npa address to the transport addresses of the gatekeepers responsible for the npa. Translates called E.164 to the transport address (TA) of responsible remote Gatekeeper. The are 2 options to consider: • The network gatekeeper queries the remote gatekeeper to get the TA of the remote Gateway, to then return it to the querying gatekeeper or, • The network gatekeeper returns the TA of the remote gatekeeper to the querying gatekeeper, which is then responsible to do the follow-up query.

Gatekeeper/Gateway functionality Breakdown

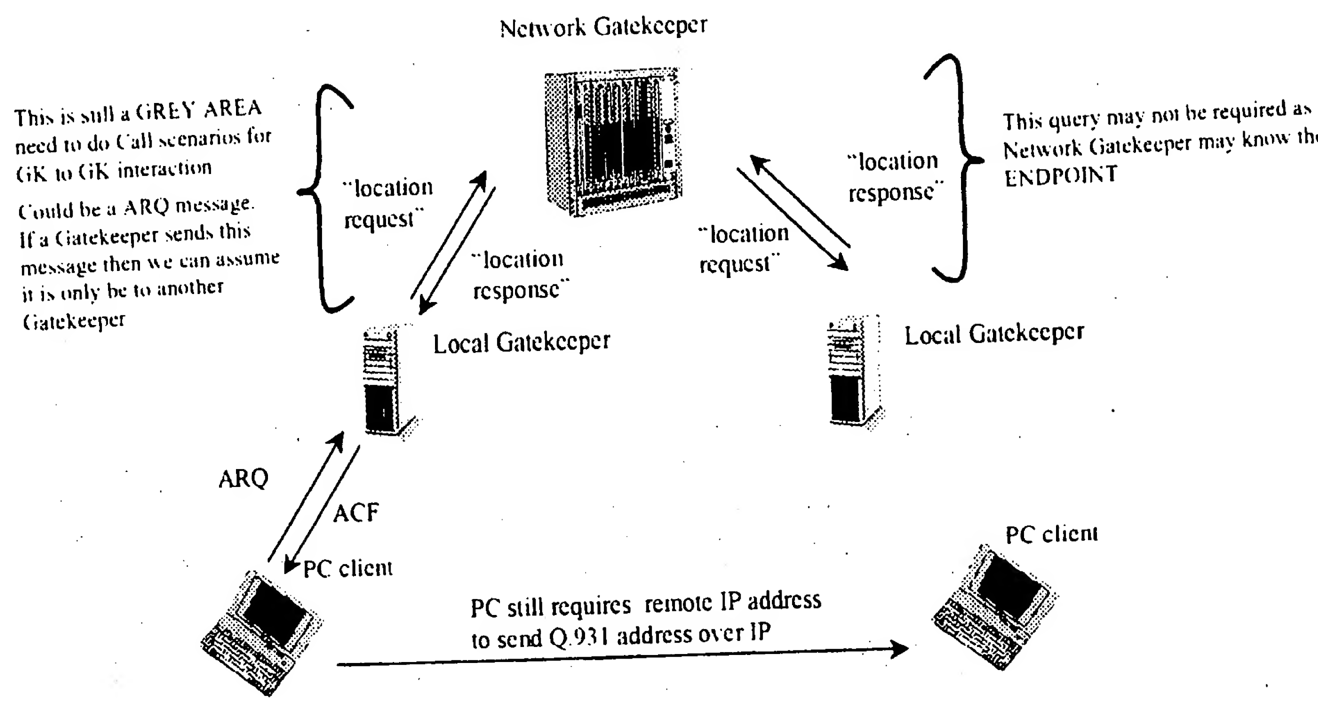
Functionality	Gateway/MMCS	Local Gatekeeper/MMCS	Network Gatekeeper
Admission Control	N/A	All Gateways must register with local Gatekeeper. IP terminals must register with local gatekeeper supplying its transport address and E.164 address. Receives admission request from endpoints (gateway or IP terminals) and authorizes the calls or not.	N/A
Bandwidth Control	N/A	Must handle Bandwidth request messages but in release 1 will most likely accept anything (tbd).	Must handle Bandwidth request messages but in release 1 will accept anything (tbd).
Call Control Signalling (H.225.0)	The Gateway is responsible for handling and routing all the call control signalling between itself and the endpoint. If the Gateway is the ENDPOINT of the IP call (i.e. terminates the IP call network to access the voice network), then it is responsible for the H245 signalling and the RTP control and data channel.	N/A	N/A

Gatekeeper/Gateway functionality Breakdown

Functionality	Gateway/MMCS	Local Gatekeeper/MMCS	Network Gatekeeper
Call Authorization/Access	MMCS Class of Service will be used when and where applicable (tbd).	Perform endpoint authentication.	Perform endpoint authentication.
Bandwidth Management	MMCS will do the Resource Management.	TBD	TBD
Call Management Services	Gateway is responsible for tracking all active calls as it is also responsible for generating Call Detail Records.	N/A	N/A
Supplementary Services	Handled by GW/MMCS	N/A	N/A

Gatekeeper Cloud Hierarchy

Assumptions:
1 gatekeeper per MMCS
The gatekeeper to gatekeeper interaction requires clarification.



Possibilities of Supplementary services on Gatekeeper

The Gatekeeper may also be used as a Call Server type device to handle supplementary features, this does require work on the Gatekeeper and also may require the gatekeeper to route calls (see the call forward scenarios for call forward no answer):

- CLID → Gatekeeper involvement possibly in routed calls scenarios only, used as a trusted node
- CLID Restriction → Gatekeeper involvement possibly in routed calls scenarios only, used as a trusted node
- Call forward: →
  - Call forward on busy, — Only for gatekeeper routed calls. Gatekeeper may act as the SERVED for call forwarding.
  - Call forward no answer; — Only for gatekeeper routed calls. Gatekeeper may act as the SERVED for call forwarding.
  - Call forward unconditional, — Gatekeeper provisioned with call forward number (I.E. Voice mail)
  - Call forward not registered — Gatekeeper provisioned with call forward number (I.E. Voice mail)
- Voice Mail for Call forward conditions → Same as the above
- Call hold → N/A
- Call transfer → Only applicable for routed calls
- Calling Name → Gatekeeper involvement possibly in routed calls scenarios only, used as a trusted node
- Multiple Ringing on DNs (MADN) → Feature needs to be implemented in Gatekeeper (not there yet)
- Multiple Line Appearance (MLA) → Feature needs to be implemented in Gatekeeper (not there yet)
- 3-way Calling or conferencing → Would require a MCU. This feature has been delayed.

Call Types

LD Bypass

	Originating	Destination	
A	P1 (PSTN1)	P5 (PSTN2)	Call Flow Scenario A
B	P1 (PSTN1)	PBX2	Call Flow Scenario A
C	PBX1	PBX2	Call Flow Scenario A
D	PBX1	P5 (PSTN2)	Call Flow Scenario A

Call Center

	Originating	Destination	
O	P4 (PSTN1)	Call Center	Call Flow Scenario O
P	Call Center	P4 (PSTN1)	Call Flow Scenario A

Reach-ability

	Originating	Destination	
E	P1 (PSTN1)	PC1	Call Flow Scenario E
G	PBX1	PC1	Call Flow Scenario E
H	PC1	P1 (PSTN1)	Call Flow Scenario H
I	PC1	PBX1	Call Flow Scenario H
F	PC1	PC2	Call Flow Scenario F
J	P1 (PSTN 1)	PC3	Call Flow Scenario E
K	PC3	P1 (PSTN1)	Call Flow Scenario H
L	PBX1	PC3	Call Flow Scenario E
M	PC3	PBX1	Call Flow Scenario H
N	PC1	PC3	Call Flow Scenario F

Call Types organized into similar scenarios

Scenarios using of 1 GW

	Originating	Destination
A	P1 (PSTN1)	P5 (PSTN2)
B	P1 (PSTN1)	PBX2
C	PBX1	PBX2
D	PBX1	P5 (PSTN2)
E	P1 (PSTN1)	PC1
G	PBX1	PC1
H	PC1	P1 (PSTN1)
I	PC1	PBX1
F	PC1	PC2

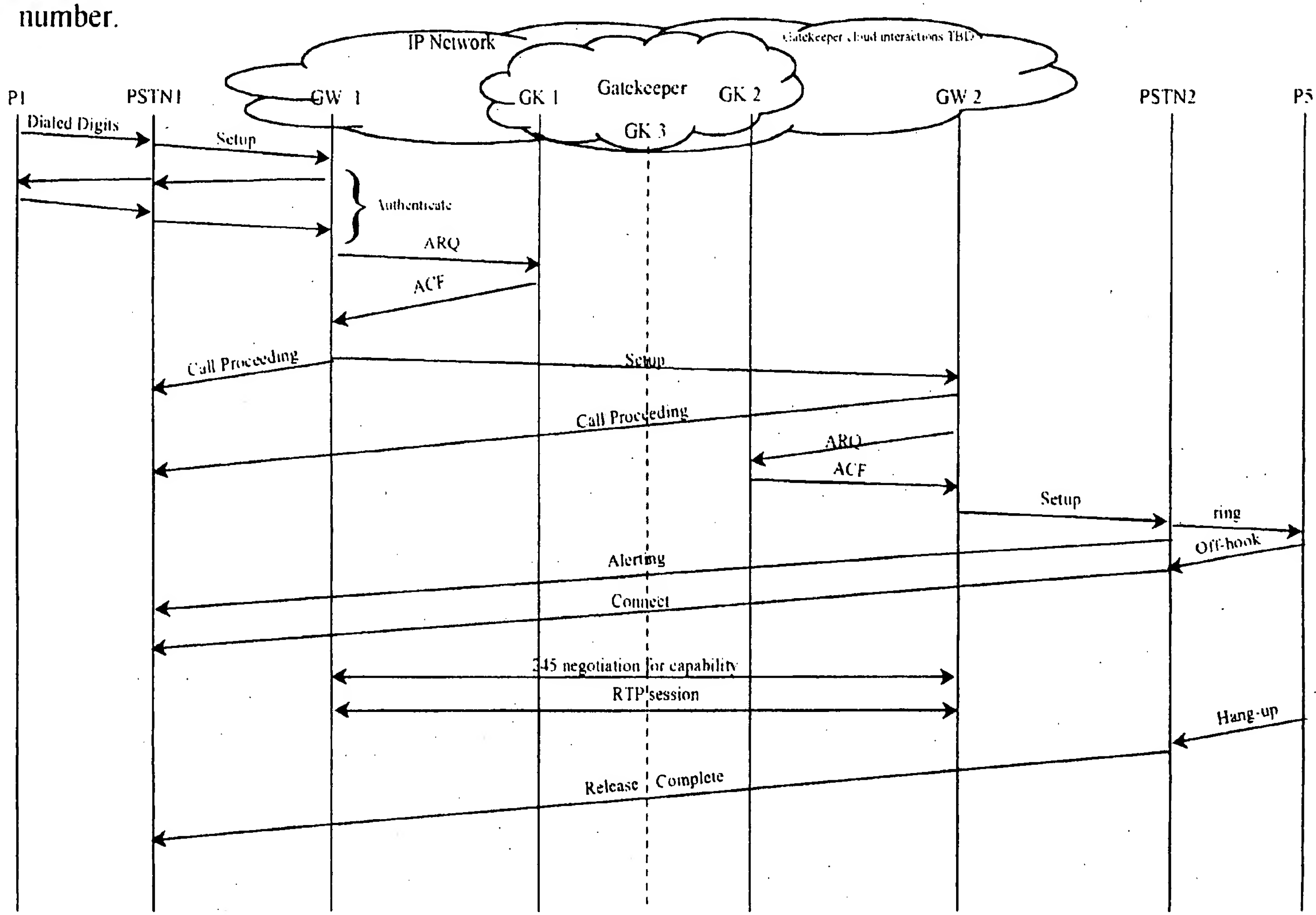
Scenarios using of 2GW

	Originating	Destination	Corresponding 1 GW scenario
O	P4 (PSTN1)	Call Center	*A*
J	P1 (PSTN 1)	PC3	*E*
L	PBX1	PC3	*G*
K	PC3	P1 (PSTN1)	*H*
M	PC3	PBX1	*I*
N	PC1	PC3	*F*

same as the connected scenario except uses 2 gateways instead of 1gateway

Scenario A: P1 (PSTN1) dials P5 (PSTN2)

Call specifics: P1 dials 1-800 number followed by authentication digits, and then P5's E.164 10-digit number.



Scenario A: P1 (PSTN1) dials P5 (PSTN2)

H.323 Gatekeeper Specific

Address Translation

- Dialed (10-digit or 15 digit?) E.164 number to transport address of terminating GW (IP address + port)

Admission Control

- No-OP since MMCS (MMCS contains the GW and local GK functionality) and does this and BW control

Bandwidth Control

- No-OP

Call Control Signalling

- Direct (handled by MMCS hence No-OP)

Call Authorization

- No-OP

Bandwidth Management (optional)

- No-OP (parked to later discussion)

Call Management

- Direct (handled by MMCS hence No-OP)

Scenario A: P1 (PSTN1) dials P5 (PSTN2)

Nortel Gatekeeper Specifics

Dialing/Numbering Plan
- E.164

Authentication of endpoints
- Parked since this issue to linked to security.

Call Routing
- No-OP handled by MMCS
-

Billing Support
- Originating Gateway/MMCS provides full support via CDR
- Terminating gateway - partial support

Credit Card / Prepaid card
- No-OP handled by MMCS. This item is an issue, please check the issue/action list.

Scenario A: P1 (PSTN1) dials P5 (PSTN2)

Supplementary Services

Call forward: Call forward on busy, Call forward no answer, Call forward unconditional,Call forward not registered
- Origination End No-OP
- Terminating End handled by PSTN

Voice Mail for Call forward conditions
- same as above

Call hold
- Originating Side -silence suppression; background noise to forward
- Terminating End - same as originating
- Q.931 ON-HOLD is not supported, we have to make a decision to add this as H.323+. Options are we could pass-thru 225 channel or for stack independent 225.0 may have to send call -hold as User Input Indication

Call transfer
- Orig side - No-OP in GW (done by PSTN)
- Term Side - No-OP in GW (done by PSTN)

3-way Calling or conferencing (Max. 1 IP device)
- same as Call transfer

CLID
- Available if present

CLID Restriction
- Handled by far-end PSTN (last node in call)

Calling Name
- No-OP

Multiple Ringing on DN (MADN)
- No-OP (handled by PSTN)

Multiple Line Appearance
- No-OP (handled by PSTN)

SCENARIO B: P1 (PSTN1) dials to PBX2

Call specifics. P1 calls a phone on PBX2
Same Call Flow as Scenario A

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario A

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario A

- No-OP all services handled by endpoint.
- Multiple Ringing on DN (MADN)
  No-OP (handled by PBX)

SCENARIO C: PBX1 dials to PBX2

Call specifics. PRI between PBX and MMCS. Phone on PBX1 calls phone PBX2

Same Call Flow as Scenario A

Note the MMCS "acts like the PSTN".

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario A

Address Translation

- E.164 to transport address terminating GW (TSAP).

Issues are as follows:

- Who does user to E,164translation
- Does PBX originating side do private # to E.164 translation.
- If MMCS based, the we use dialed number and also based on incoming trunk digits.

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario A

No-OP all services handled by endpoint.

Calling Name

- No-OP (Do we passthru) information, refer to issues/action list.

SCENARIO D: PBX1 dials to P5 (PSTN2)

<u>Call specifics.</u> PRI between PBX and MMCS. Phone on PBX1 calls P5

Same Call Flow as Scenario A

<u>H.323 Gatekeeper Specific</u>

Unless otherwise specified all solutions are the same as Scenario A (and C)

Address Translation

- E.164 only

  Issues same as Scenario C

<u>Nortel Gatekeeper Specifics</u>

Unless otherwise specified all solutions are the same as Scenario A

<u>Supplementary Services</u>

Unless otherwise specified all solutions are the same as Scenario A

SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

Call specifics.

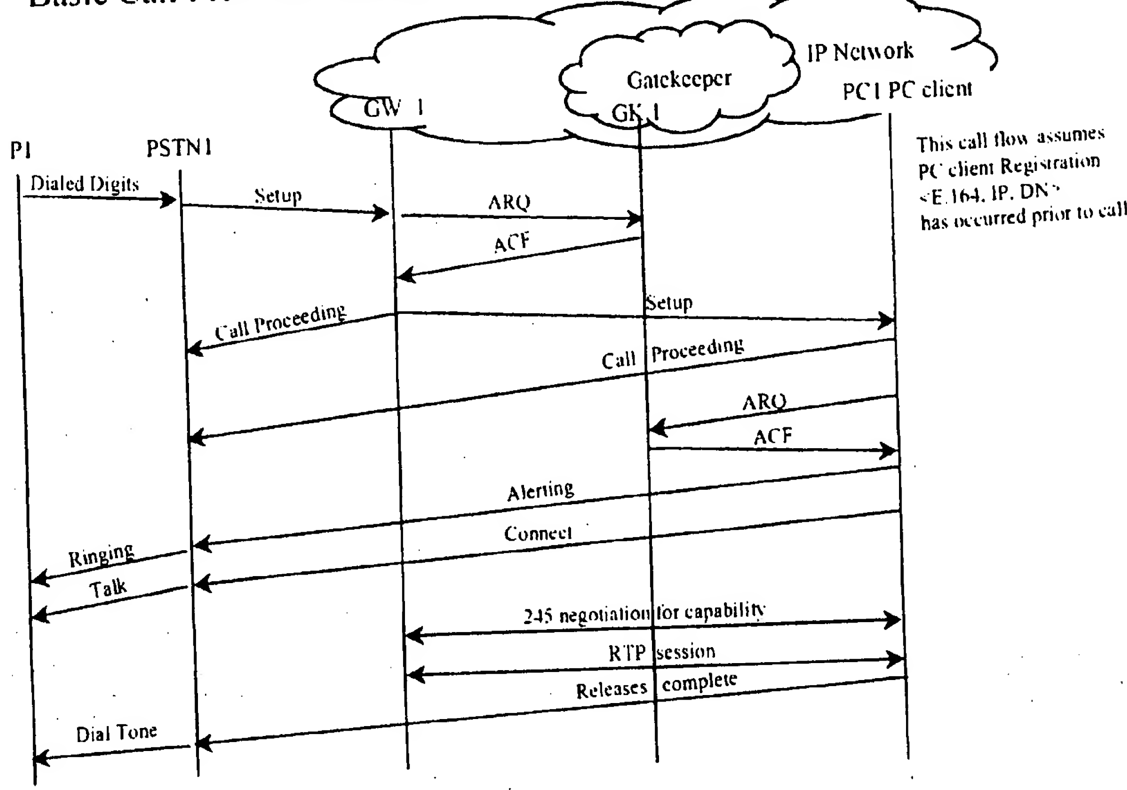
P1 dials PC1's E.164 10-digit number.

Assumptions:

Same business model DN off a centrex

- PC client has no assumption/ties with a corporate network
- Directly serviced by network service provider
- Gatekeeper handles DN, E.164, IP association

Basic Call Flow for Scenario E: P1 (PSTN1) to PC1 (Road Warrior)



SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario A Address Translation

- Need DN<>E.164<>IP address translation/association

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A
Dialing/Numbering Plan this is linked to the H.323 addressing issue

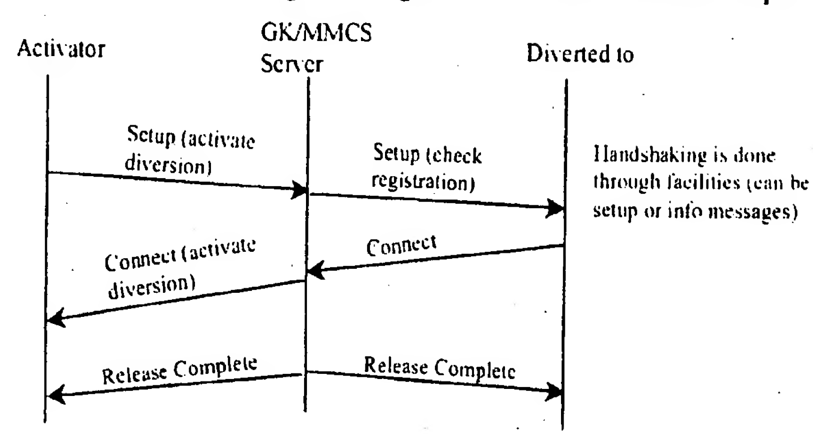
Supplementary Services

Call forward: Call forward on busy, Call forward no answer, Call forward unconditional,Call forward not registered

- Call forward Unconditional
- Assumption: If call forward is set and call tries to terminate on the forwarded number, the call will do what the default MMCS treatment does.

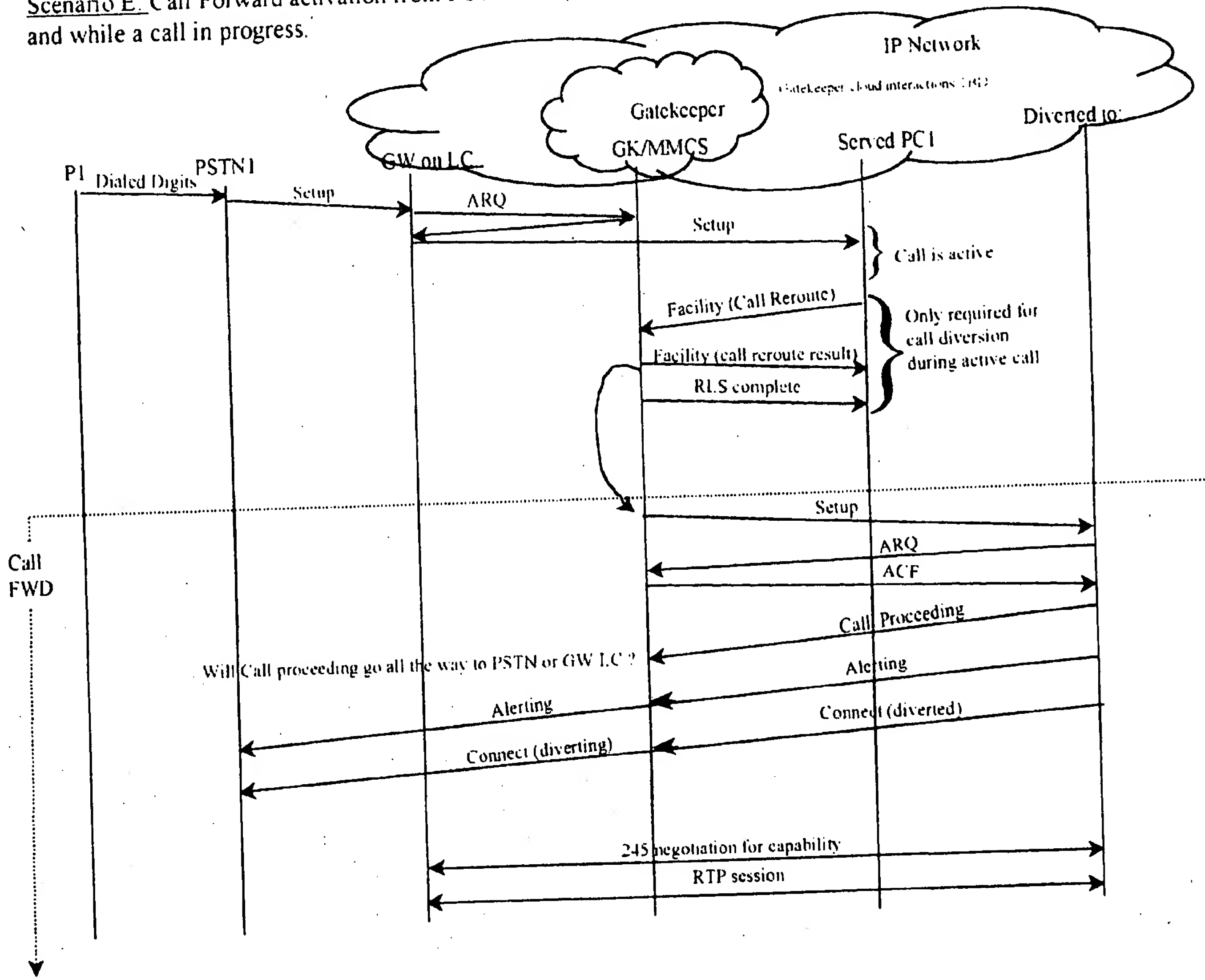
Call forward activation across the gatekeeper cloud needs to be clarified

CFU activation handshake messages for agents on the same GateKeeper



SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

Scenario E. Call Forward activation from PC1 to new terminal (diverted to) where the diverted to terminal is on the same GK, and while a call in progress.



SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

Supplementary Services (continued)

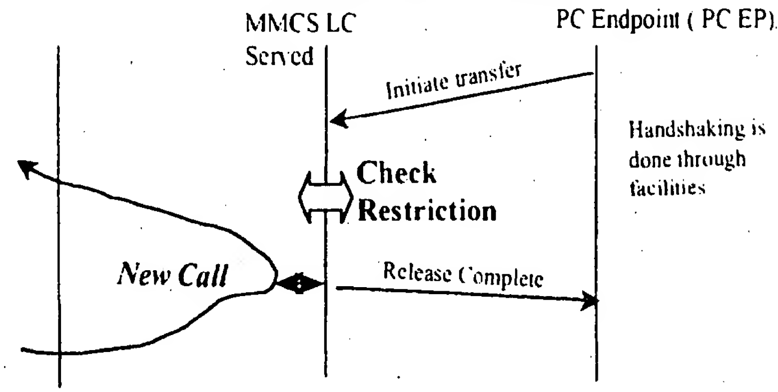
Call Hold

- Origination - handled by PSTN
- Terminating activates call hold, send userInput Indication
- NO RTP packets to GW

Call transfer

- Origination - handled by PSTN
- Terminating (refer to call flow diagram)

Call transfer activation



Note:

Double Code/Encode possible if Originating transfers to another IP/Cellular client

- Options include forcing 711 negotiation?
- Or make new call to setup and renegotiate.

SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

Supplementary Services (continued)

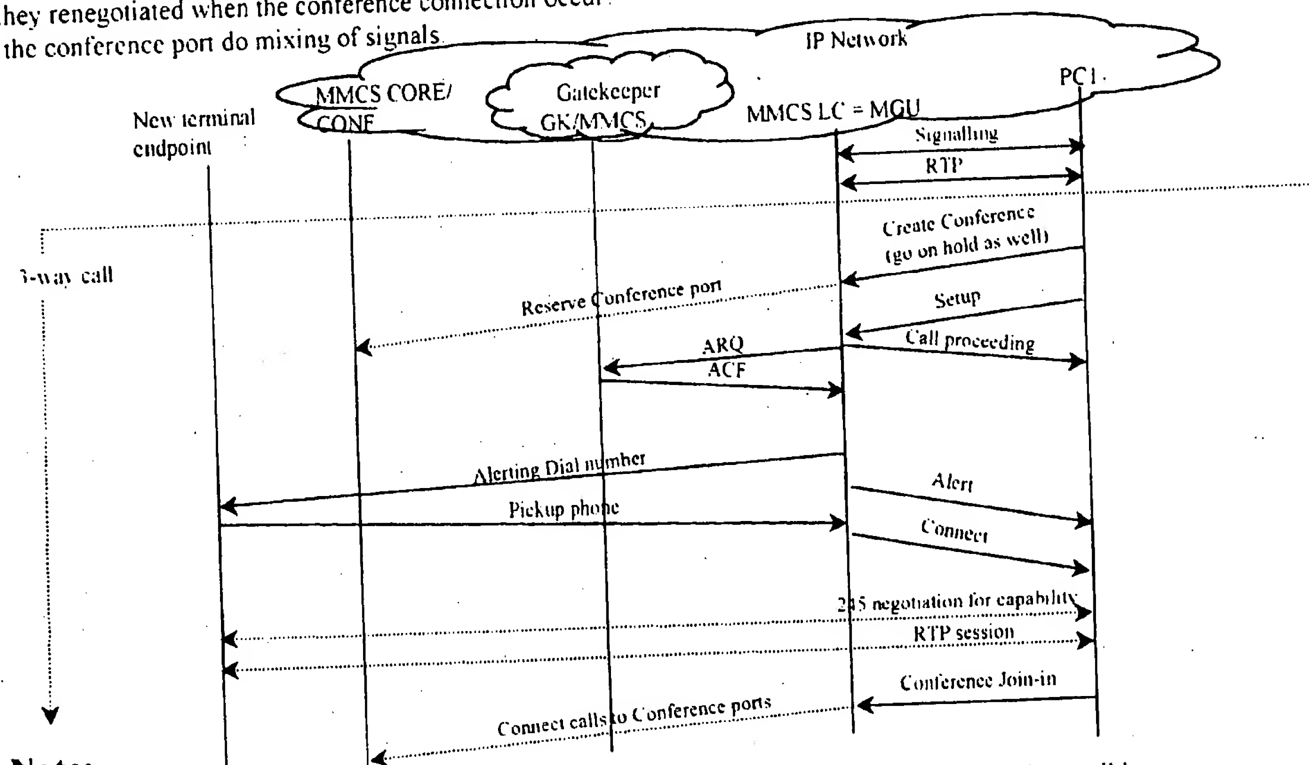
3-way call

- Origination - handled by PSTN
- Terminating (refer to call flow diagram)

Call up between PC1 and other phone. PC1 initiates a conference call to New terminal endpoint

Questions

- When PC1 connects to the new terminal are the H245 signalling /RTP negotiated before bridging the conference ?
- Are they renegotiated when the conference connection occur?
- Will the conference port do mixing of signals.



Note:

- Can We renegotiate for voice quality and as in the call transfer case, double compression is possible.
- Are line CDRs generated for station to station calls?

SCENARIO E: P1 (PSTN1) dials to PC1 (Road Warrior)

Supplementary Services (continued)

CLID

- Origination - No OP handled by PSTN
- NO ISSUES

CLID Restriction

- NO ISSUES MMCS/PSTN handled

CALLING NAME

- NO ISSUES MMCS/PSTN handled

MADN

- Assumption All DNs on the same MMCS node/GK
- TO BE DESIGNED?

Multiple Line Appearance

- On legacy only using one codec at one time, infers that only one call up at a time ?

SCENARIO F: PC1 (Road Warrior) dials to PC2 (Road Warrior)

Call specifics.

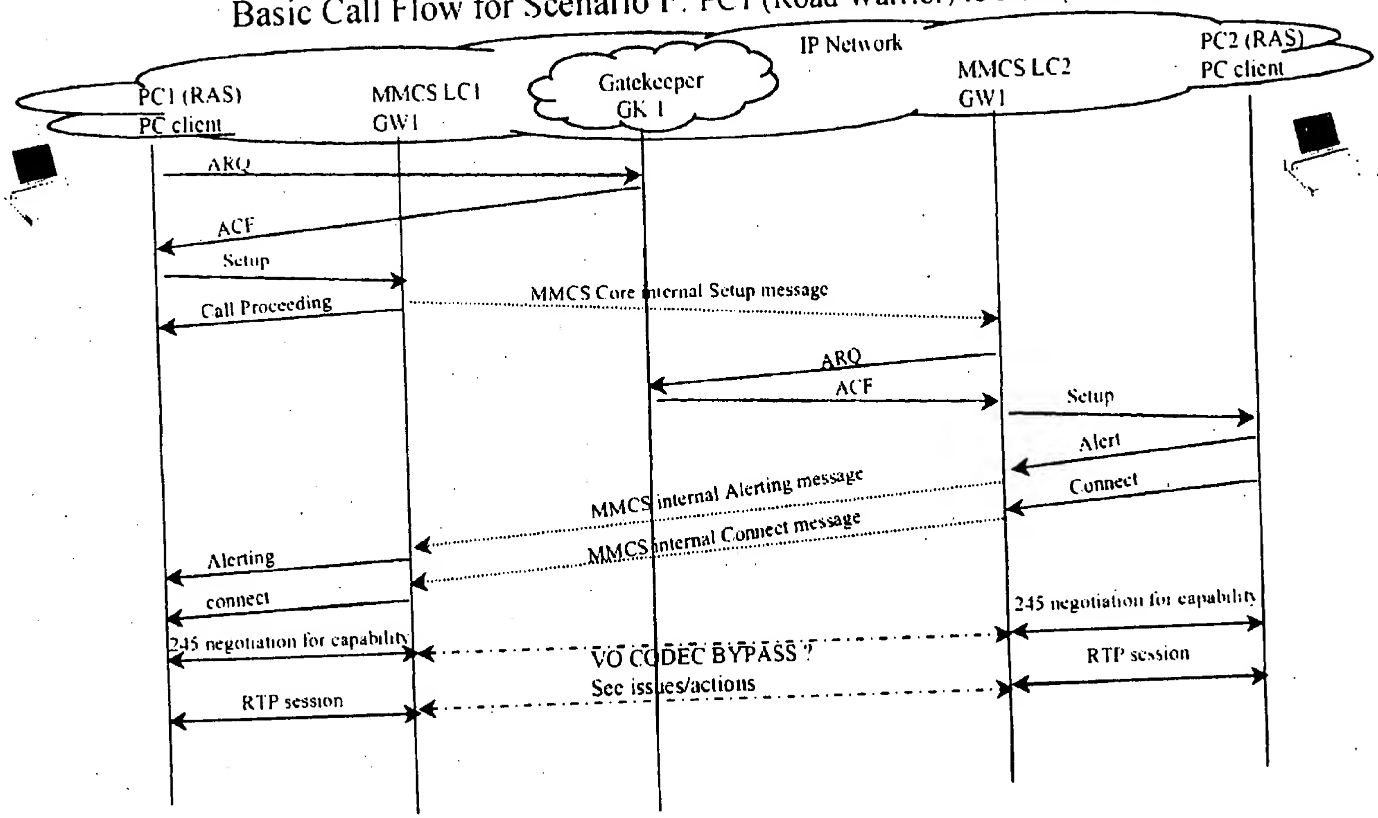
Assumptions:

Same business model DN off a centrex and this is an IP to IP call

- PC client has no assumption/ties with a corporate network
- Directly services by network service provider
- DN, E.164, IP association

Dialed Digits

Basic Call Flow for Scenario F: PC1 (Road Warrior) to PC2 (Road Warrior)



SCENARIO F: PC1 (Road Warrior) dials to PC2 (Road Warrior)

Potential problems

Possible problems are:

- What if there are 2 different codecs on 2 legs.
- Possible Voice Quality issues on dialup IP clients
- Need for VO CODEC bypass

We want a Road warrior concept to be applicable at home or on the road, ie. Single DN. This creates certain routing problems

- option is to always route through the MMCS

H.323 Gatekeeper Specific

Address Translation

Unless otherwise specified all solutions are the same as Scenario A

- E.164 to transport address terminating GW (TSAP)

Admission Control

- Post Registration/Treatment of ARQ (handled by MMCS/GK)

Bandwidth Control

- same as above (handled by MMCS/GK)

Call Control Signalling

- same as above (handled by MMCS/GK)

Call Authorization

- same as above (handled by MMCS/GK)

Bandwidth Management (optional)

- same as above (handled by MMCS/GK)

Call Management

- same as above (handled by MMCS/GK)

SCENARIO F: PC1 (Road Warrior) dials to PC2 (Road Warrior)

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A

Supplementary Services

REFER TO MAYEUL's charts in Appendix A.

Call forward:
- refer to Scenario E, IP terminal
- double compression possible

Voice Mail for Call forward conditions
- refer to Scenario E, IP terminal
- double compression possible

Call hold
- refer to Scenario E, IP terminal

Call transfer
- refer to Scenario E, IP terminal

3-way Calling or conferencing (Max. 1 IP device)
- Origination from PC1, refer to Scenario E, IP terminal CLID
- Available if present

CLID Restriction
- Handled by far-end PSTN (last node in call)

Calling Name
- MMCS handled, extra development required to send PC name (this is different from the datafilled name in the switch).

Multiple Ringing on DN (MADN)
- refer to Scenario E, IP terminal

Multiple Line Appearance
- refer to Scenario E, IP terminal

SCENARIO G: PBX1 dials to PC1 (Road Warrior)

Call specifics.

Same Call Flow as Scenario E

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario E Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario E

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario E

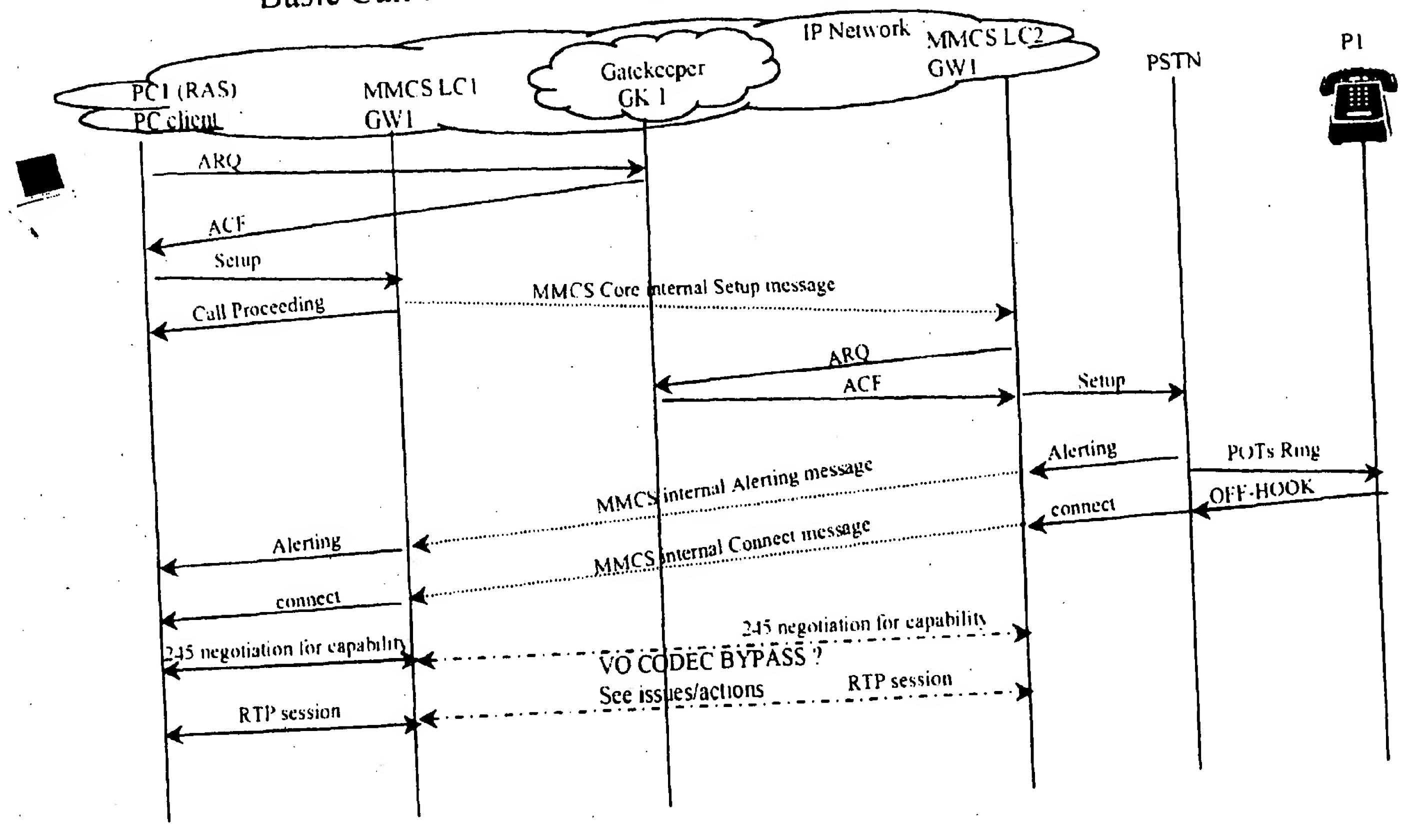
SCENARIO H: PC1 dials to P1 (PSTN1)

Call specifics.

Same business model DN off a centrex and this is an IP to IP call

- PC client has no assumption/ties with a corporate network
- Directly services by network service provider
- DN, E.164, IP association

Basic Call Flow for Scenario H: PC1 (Road Warrior) to P1 (PSTN1)



SCENARIO H: PC1 dials to P1 (PSTN1)

Potential problems

Possible problems are:

- Possible Voice Quality issues on dialup IP clients

We want a Road warrior concept to be applicable at home or on the road, ie. Single DN. This creates certain routing problems.

- option is to always route through the MMCS

H.323 Gatekeeper Specific

Address Translation

Unless otherwise specified all solutions are the same as Scenario A

- E.164 to transport address terminating GW (TSAP)

Admission Control

- Post Registration/Treatment of ARQ (handled by MMCS/GK)

Bandwidth Control

- same as above (handled by MMCS/GK)

Call Control Signalling

- same as above (handled by MMCS/GK)

Call Authorization

- same as above (handled by MMCS/GK)

Bandwidth Management (optional)

- same as above (handled by MMCS/GK)

Call Management

- same as above (handled by MMCS/GK)

SCENARIO H: PC1 dials to P1 (PSTN1)

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A

Supplementary Services

Call forward:
- refer to Scenario E, IP terminal
- double compression possible

Voice Mail for Call forward conditions
- refer to Scenario E, IP terminal
- double compression possible

Call hold
- refer to Scenario E, IP terminal

Call transfer
- refer to Scenario E, IP terminal

3-way Calling or conferencing (Max. 1 IP device)
- Origination from PC1, refer to Scenario E, IP terminal CLID
- Available if present

CLID Restriction
- Handled by far-end PSTN (last node in call)

Calling Name
- MMCS handled, extra development required to send PC name (this is different from the datafilled name in the switch).

Multiple Ringing on DN (MADN)
- refer to Scenario E, IP terminal

Multiple Line Appearance
- refer to Scenario E, IP terminal

SCENARIO I: PC1 (Road Warrior) dials to PBX1

Call specifics.

Same Call Flow as Scenario H

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario H Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario H

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario H

SCENARIO J: P1 (PSTN) dials to PC3 (2GWs)

Call specifics.

Same Call Flow as Scenario E.

For scenarios J to M it is assumed that the ***PC clients are associated with a gateway***. Hence the supplementary features work in the indicated for originating/terminated fashion as shown in previous call flows (I.E. handled by PSTN, PBX or MMCS if the activating terminal in on the PSTN, PBX or PC terminal respectively)

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario E Address Translation

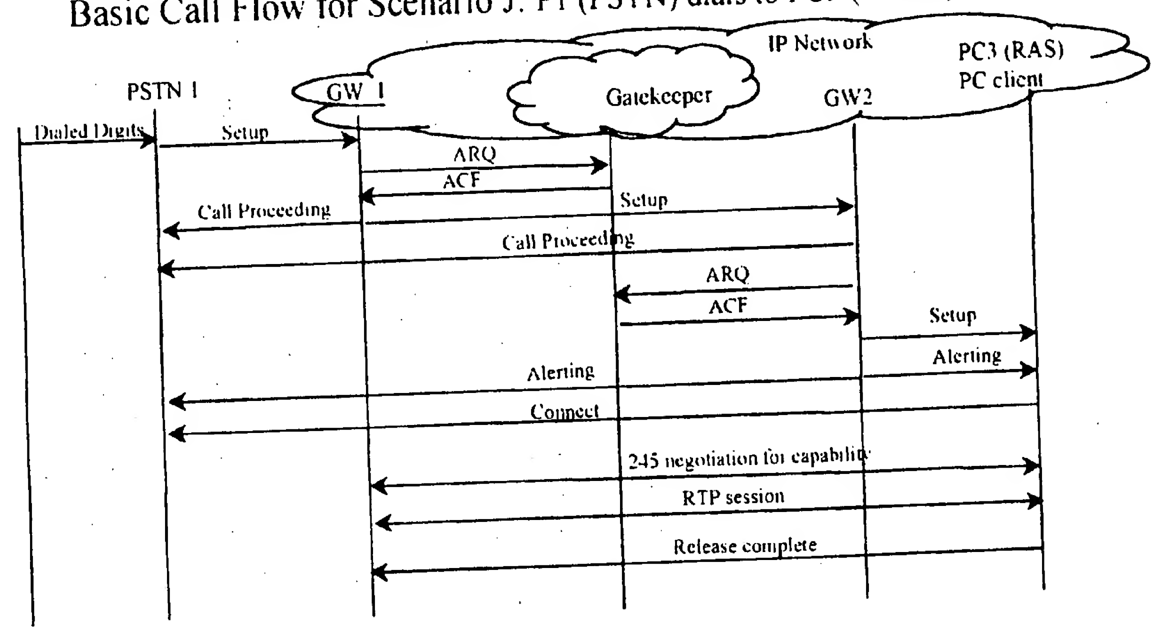
Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario E

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario E

Basic Call Flow for Scenario J: P1 (PSTN) dials to PC3 (2GWs)



SCENARIO K: PC3 (Road Warrior) dials to P1 (PSTN1) - 2GWs

Call specifics.

Same Call Flow as Scenario H except has 2 Gateways

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario H Address Translation

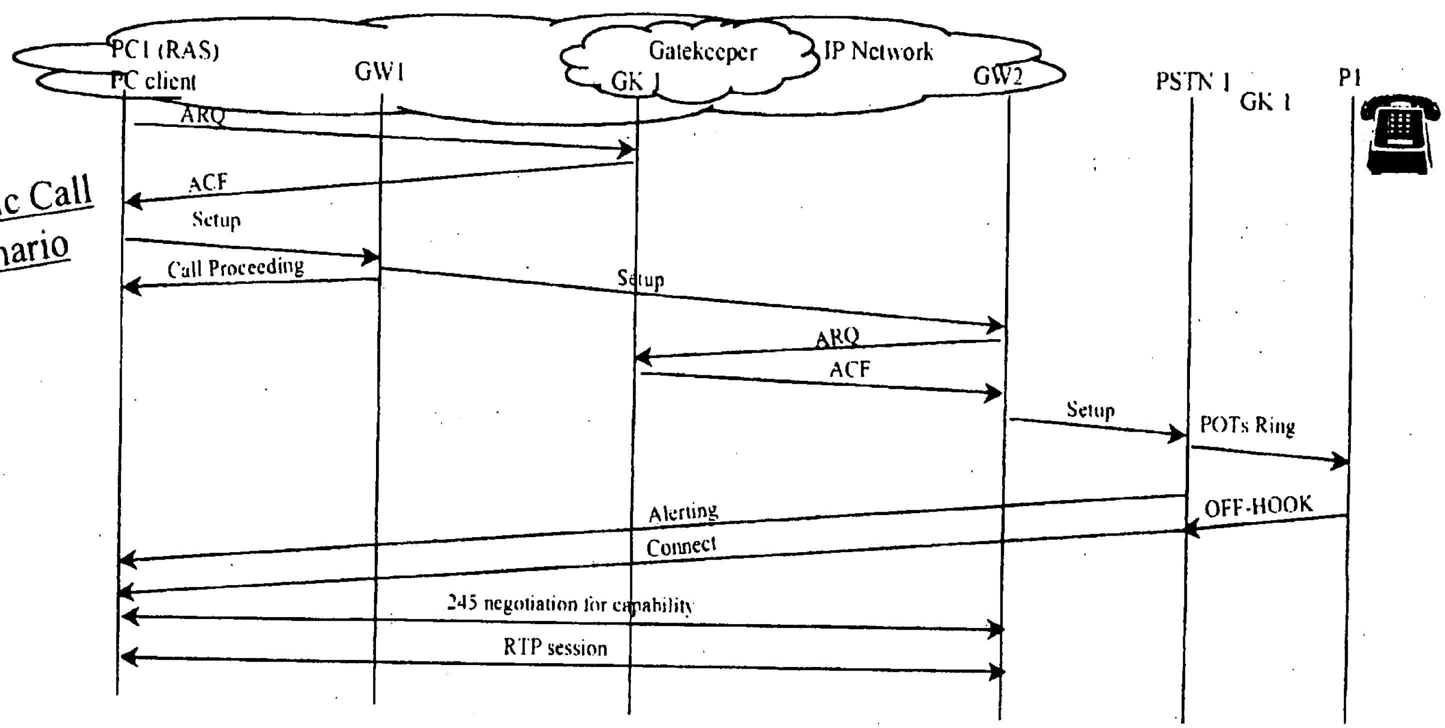
Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario H

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario H

Basic Call scenario



SCENARIO L: PBX1 dials to PC3 - 2GWs

Call specifics.

Same Call Flow as Scenario J

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario E Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario E

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario E

SCENARIO M: PC3 (Road Warrior) dials to PBX1 - 2GWs

Call specifics.

Same Call Flow as Scenario K

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario H Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario H

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario H

SCENARIO N: PC1 dials to PC3 - 2GWs

Call specifics.

Same Call Flow as Scenario F except 2 gateways are present.

H.323 Gatekeeper Specific

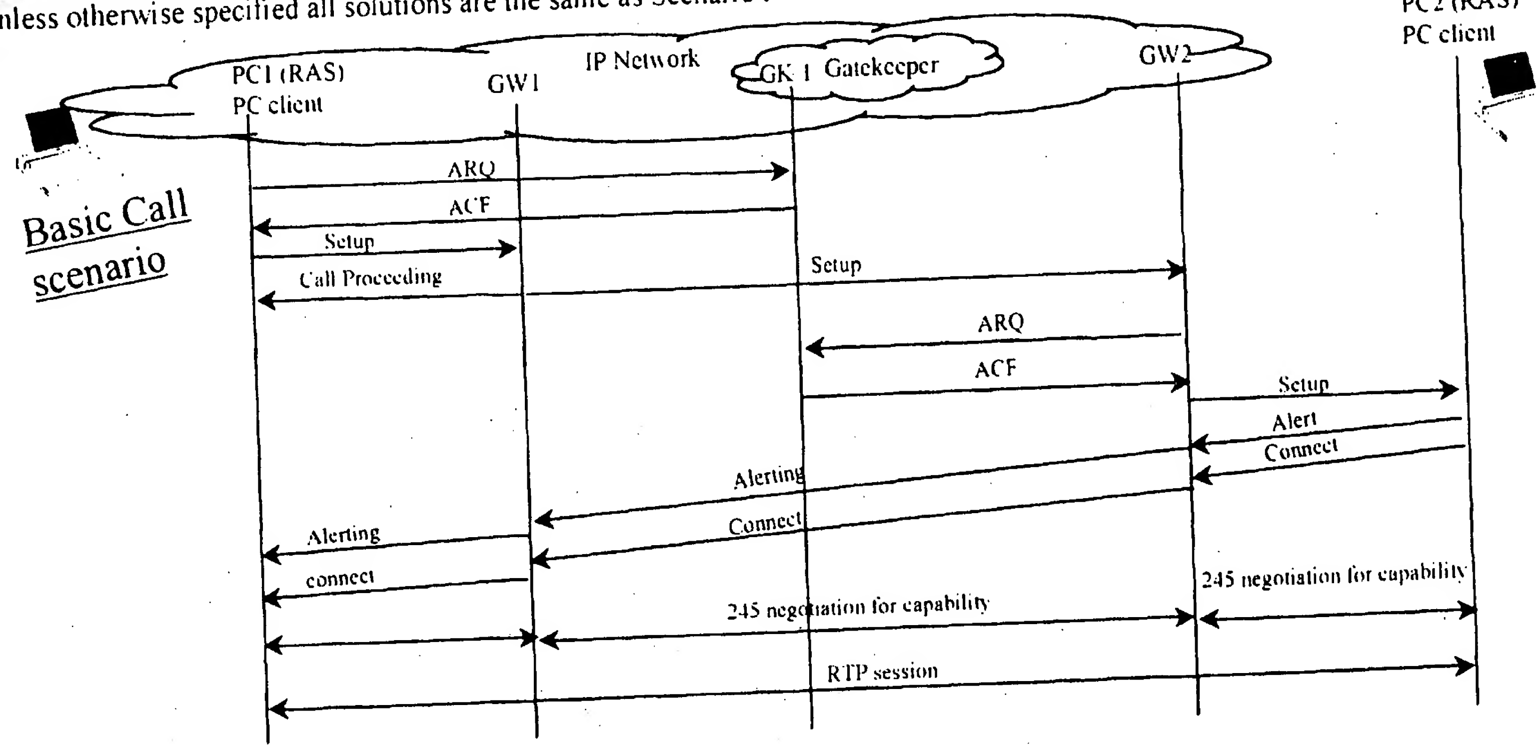
Unless otherwise specified all solutions are the same as Scenario F Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario F

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario F



SCENARIO O: P4 (PSTN) dials to Call Center - 2GWs

Call specifics.

Same Call Flow as Scenario A

The local GK/network (a breakdown of the network/local gatekeeper functionality are presently being defined as part of the issues) must know of where the remote call centre is located and hence translated the local call to the long distance call digits. Otherwise the call scenario is the same as Scenario A.

There is an issue on where the billing is done since from the originating side this is a local call and hence should not be billed. However since the originating side generates a CDR for this call this is not a problem as these records are compiled and sent to the call centre.

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario A Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario A

Billing Support

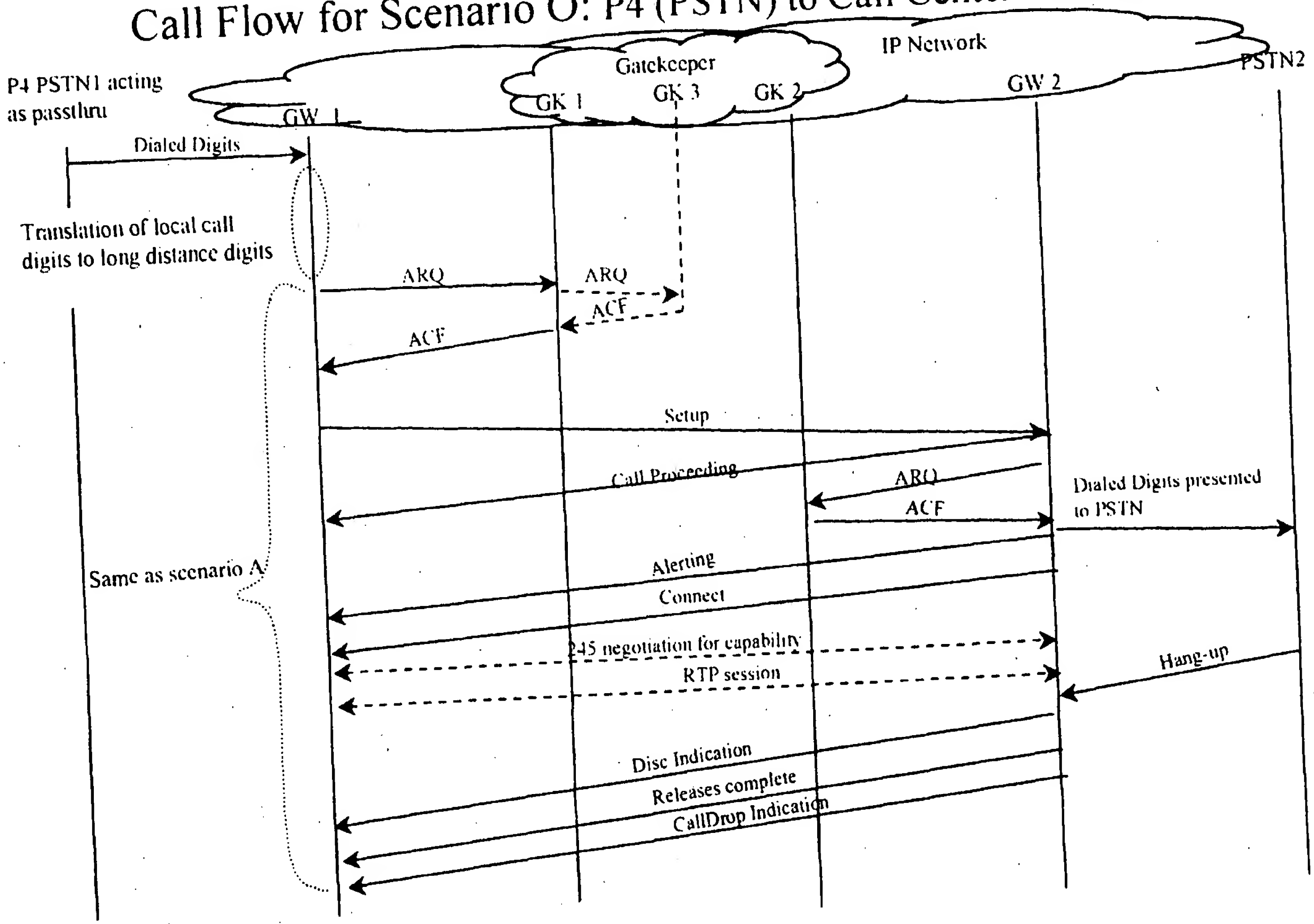
- Originating Gateway/MMCS provides full support via CDR
- Terminating gateway - partial support

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario A

SCENARIO O: P4 (PSTN) dials to Call Center - 2GWs

Call Flow for Scenario O: P4 (PSTN) to Call Center - 2GWs



SCENARIO P: Call Center dials to P4 (PSTN) - 2GWs

Call specifics.

Same Call Flow as Scenario D (which is itself the same as scenario A).

H.323 Gatekeeper Specific

Unless otherwise specified all solutions are the same as Scenario D Address Translation

Nortel Gatekeeper Specifics

Unless otherwise specified all solutions are the same as Scenario D

Supplementary Services

Unless otherwise specified all solutions are the same as Scenario D

Appendix 2:

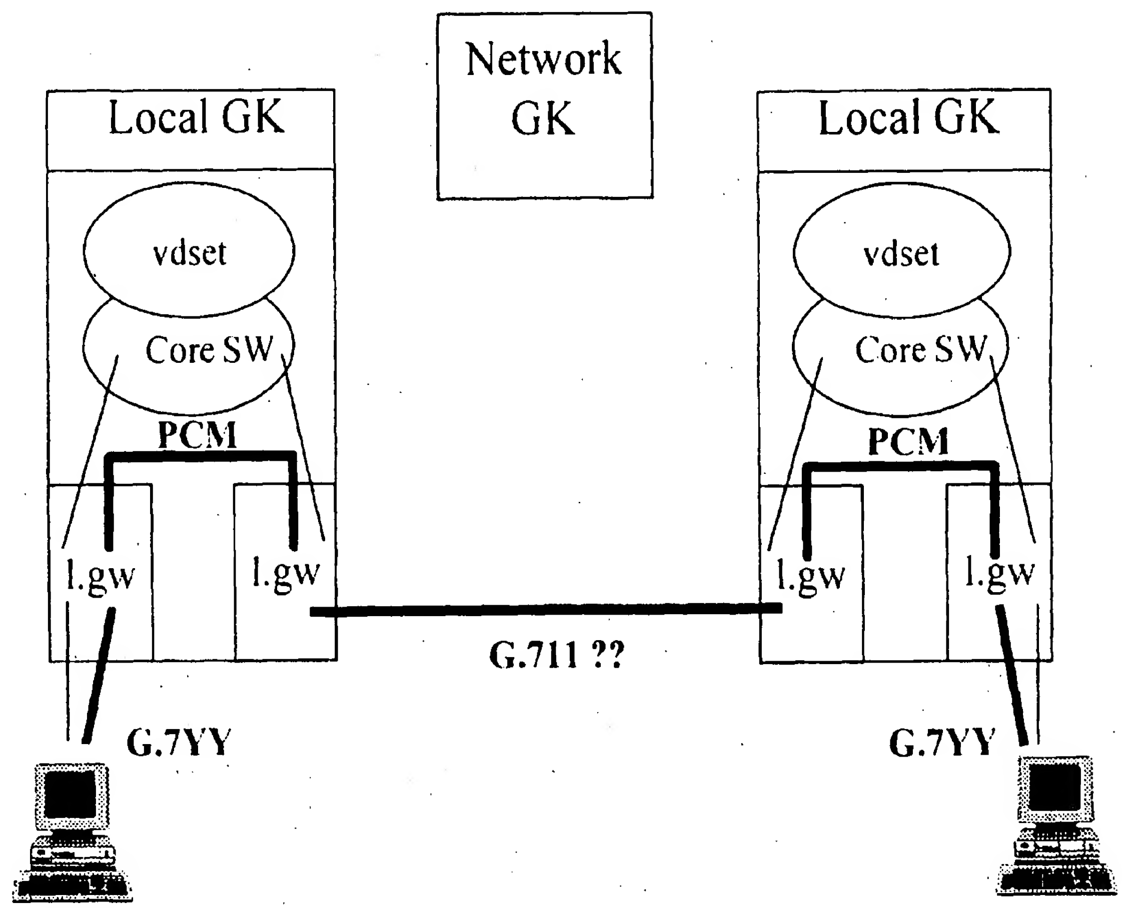
IP TELEPHONY GATEWAY

Appendix A: Mayeul's Call-Flow presentation

<u>Connection between 2 PC terminal using the same or different compression algorithms</u>

2 GWs and 2 GKs (may/may not have used the Network GateKeeper to establish connection depending on Zone division)

Diagram shows an established connection & how double compression is possible.

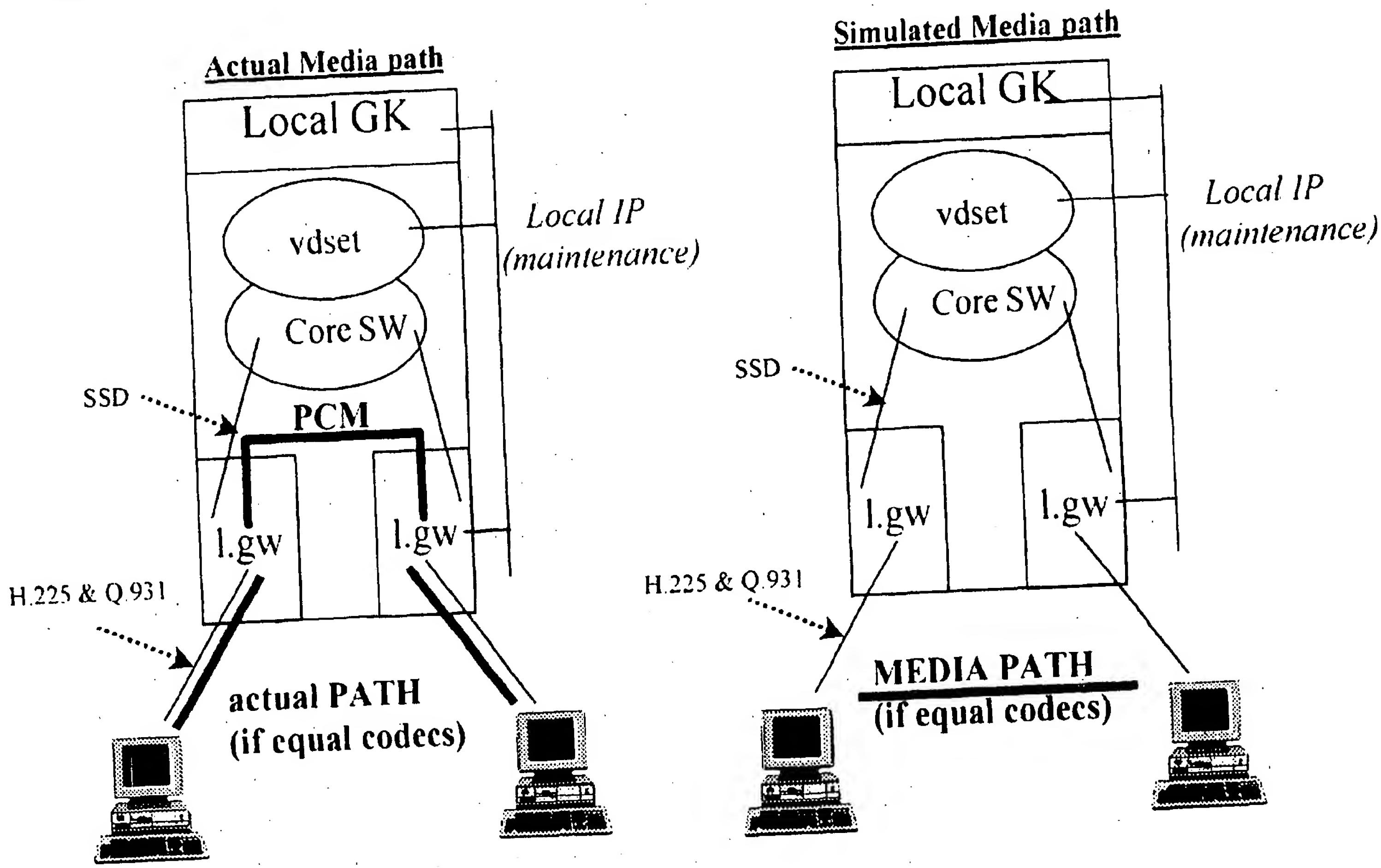


Appendix A: Mayeul's Call-Flow presentation

Connection between 2 PC terminal using the same compression algorithms

2 GWs and 1 GKs

Diagram shows an established connection with no double compression.

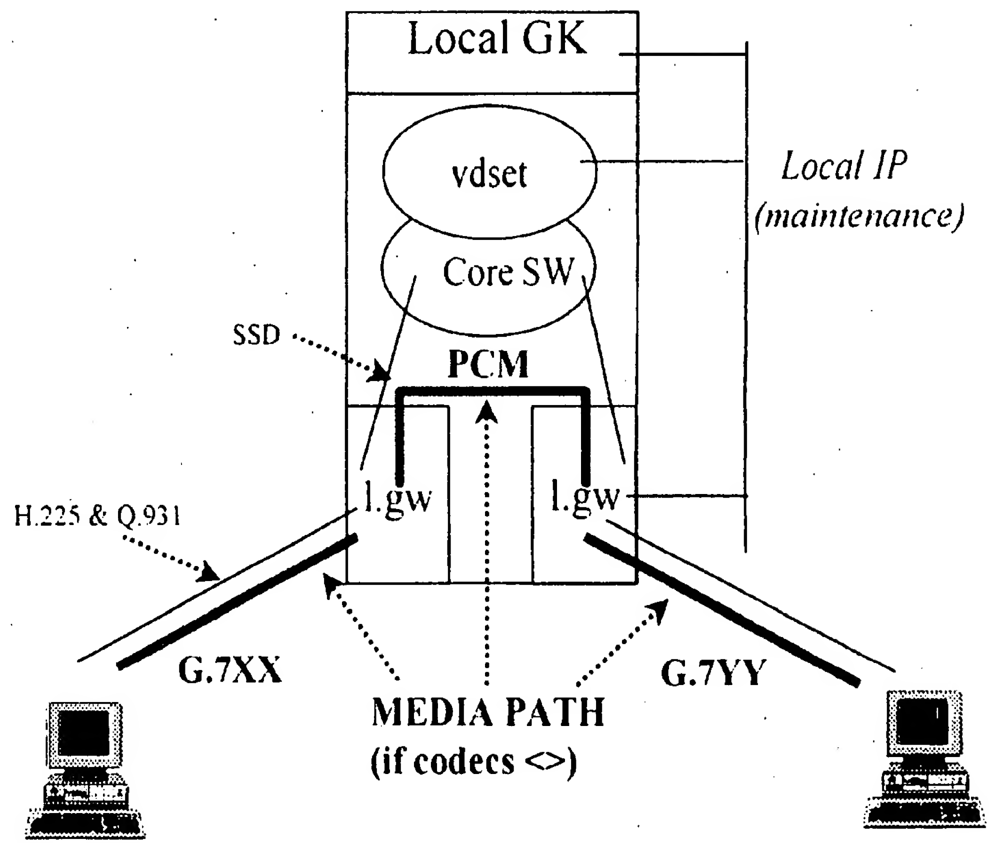


Appendix A: Mayeul's Call-Flow presentation

Connection between 2 PC terminal using the different compression algorithms

2 GWs and 1 GKs

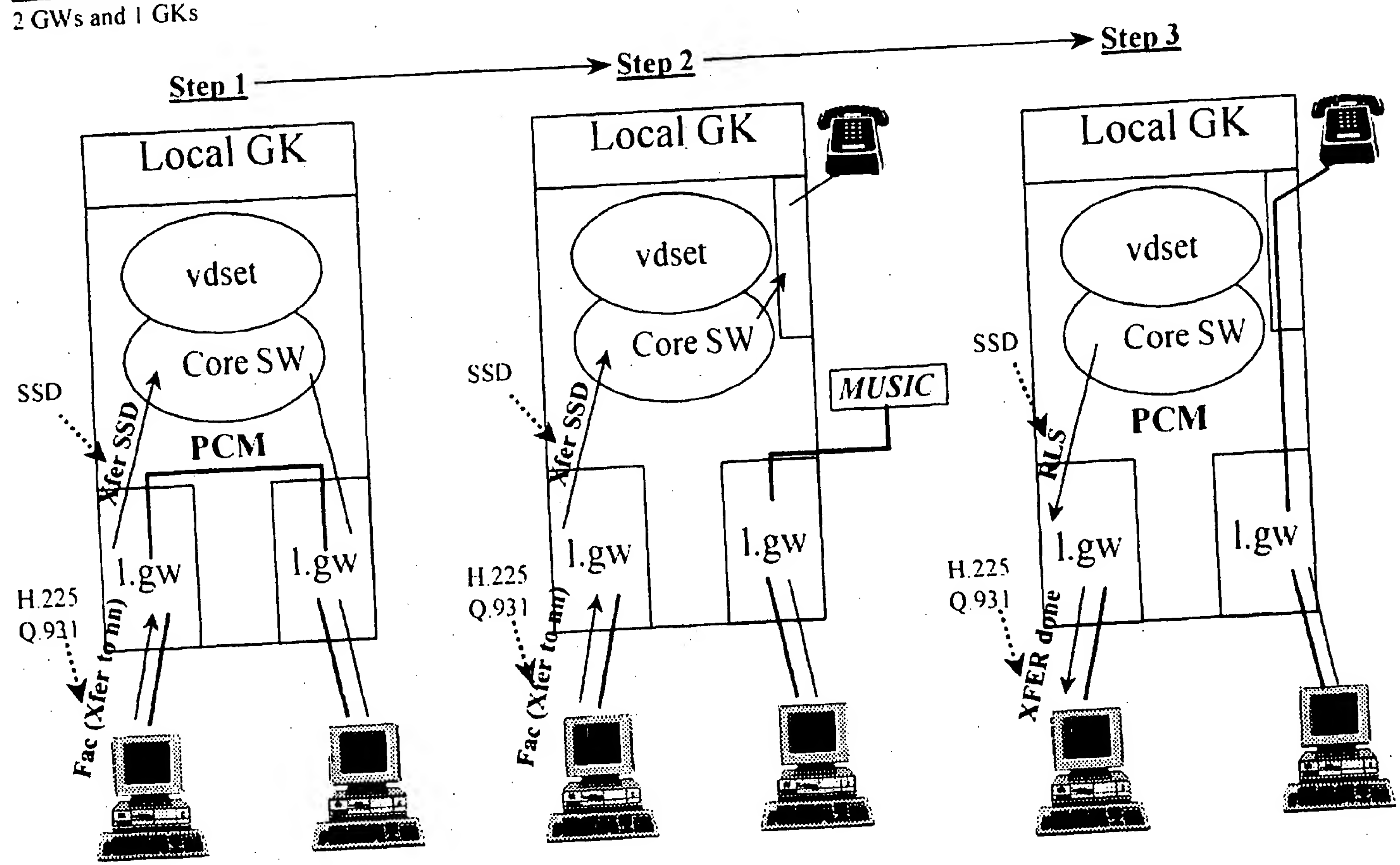
Diagram shows an established connection with possible double compression



Appendix A: Mayeul's Call-Flow presentation

Transfer Call Scenario

2 GWs and 1 GKs



Appendix 3:

IP TELEPHONY GATEWAY

Supplementary Services on IP terminals

Originating Terminal	Terminating Terminal
Call Hold: Option is to pass in as part of UUIE field in UserInputIndicaton which allows a non-standard parameter to be added (using the **NonStandardParameter** field in the ASN.1 file). This is not part of the H.323/H245 standard and would require client work to initiate a call hold UUIE element.	Call Hold: Same as on the originating side.
CLID: This supplementary feature is not part of the H225/H245 standard. As with the Call Hold service, can be part of the UserInputIndication but again would require work on the clients.	CLID: Client would require work to display UUIE UserInputIndication data.
Calling Name: Same reasoning as CLID	Calling Name: Client would require work to display UUIE UserInputIndication data.
CLID Restriction: Work required to client to add this to the UUIE field.	CLID Restriction: Calling Party number can be stripped at the client (this is a security and privacy problem) or can be stripped at the MMCS (assuming that the call signalling is done by MMCS).

Note1: Call Hold/CLID/Calling Name are facility IE's in Setup messages in Q.931and are not part of the H.225 standard. Modifying the Setup Message to support this work require work with the standards bodies and with the PC client software. Adding these facilities as part of the UserInputIndication stills requires client work, however the UUIE field is considered data.

Note2: The above calls are assuming IP to IP calls. If the originating or terminating end call is a PSTN or PBX phone, then the gateway would be responsible adding the UserInputIndication as required.

Originating Terminal	Terminating Terminal
MADN: Not Applicable.	MADN: Limited to the same Gateway if implemented feature is part of the MMCS. Gatekeeper handles MADN call control. This requires additional work on the Gatekeeper but MADN would no longer be limited to one gateway.
MLA: No Additional work required at Gatekeeper. On originating side this would be considered as a single line initiating a call.	MLA: Additional work required at Gatekeeper as in the case administrator being able to pickup their bosses phone. Call signalling must passthru the gatekeeper initially for Setup and Connect message. Gatekeeper must issue multiple Setup messages on behalf of the Calling party and arbitrate which of the terminating agents gets the call upon call pickup.
CFNA/CFU/CFU: The originating terminal upon calling the call forwarded agent, will receive a Setup & Facility messages from the server (gateway or gatekeeper handling the call forward) or the terminating terminal and will initiating a new call to the diverted to terminal. The originating terminal must be 450.3 compliant.	CFNA/CFU/CFU: To Initiate a call forward the IP terminal must be a H450.3 compliant agent I.E. To initiate Call forward (call diversion) the Application Protocol Data Unit is sent as part of the UUIE section of the setup message. This message can be set to the Gateway, gatekeeper or not at all (in which case the terminating terminal responds to a calling agent with the rerouting information but this would be difficult to collect billing information). The diverted to terminal or gateway also needs to respond to the call forward activation with a activateDiversionQ.returnResult.

Originating Terminal	Terminating Terminal
Call XFER: IP terminal issues a transfer via a Q.931 Facility message and the APDU InitiateInvoke is part of the UUIE. IP terminal must be H450.2 compliant.	Call XFER: On receiving the InitiateInvoke the terminating terminal must initiate a new call to the transferred to terminal. IP terminal must be H450.2 compliant

Note: To Activate Call forward or Call Transfer from a IP terminals, these terminals must be H450.3 and 450.2 compliant.

Supplementary services for originating terminals or terminating terminals on the PSTN and PBX can be handled the PSTN or PBX respectively I..E. MADN and MLA. The only exceptions to this is that work will be required at the Gateways to transfer the CLID, CLID restriction and the Calling name in the UUIE UserInputIndication.

In the Call forward and Call Transfer scenarios following the messages are between IP terminal and IP terminal actions.

If an IP terminal invokes a supplementary service action such as call transfer/call forward (referred to as diverted to/reroute in H450.3 and H450.2) to a POTS phone on the PSTN (or PBX). Then the Gateway will handle the transfer/call forward message on behalf of the POTS phone. If the call transfer is initiated on the PSTN side then the PSTN will handle the call forward and call transfer.

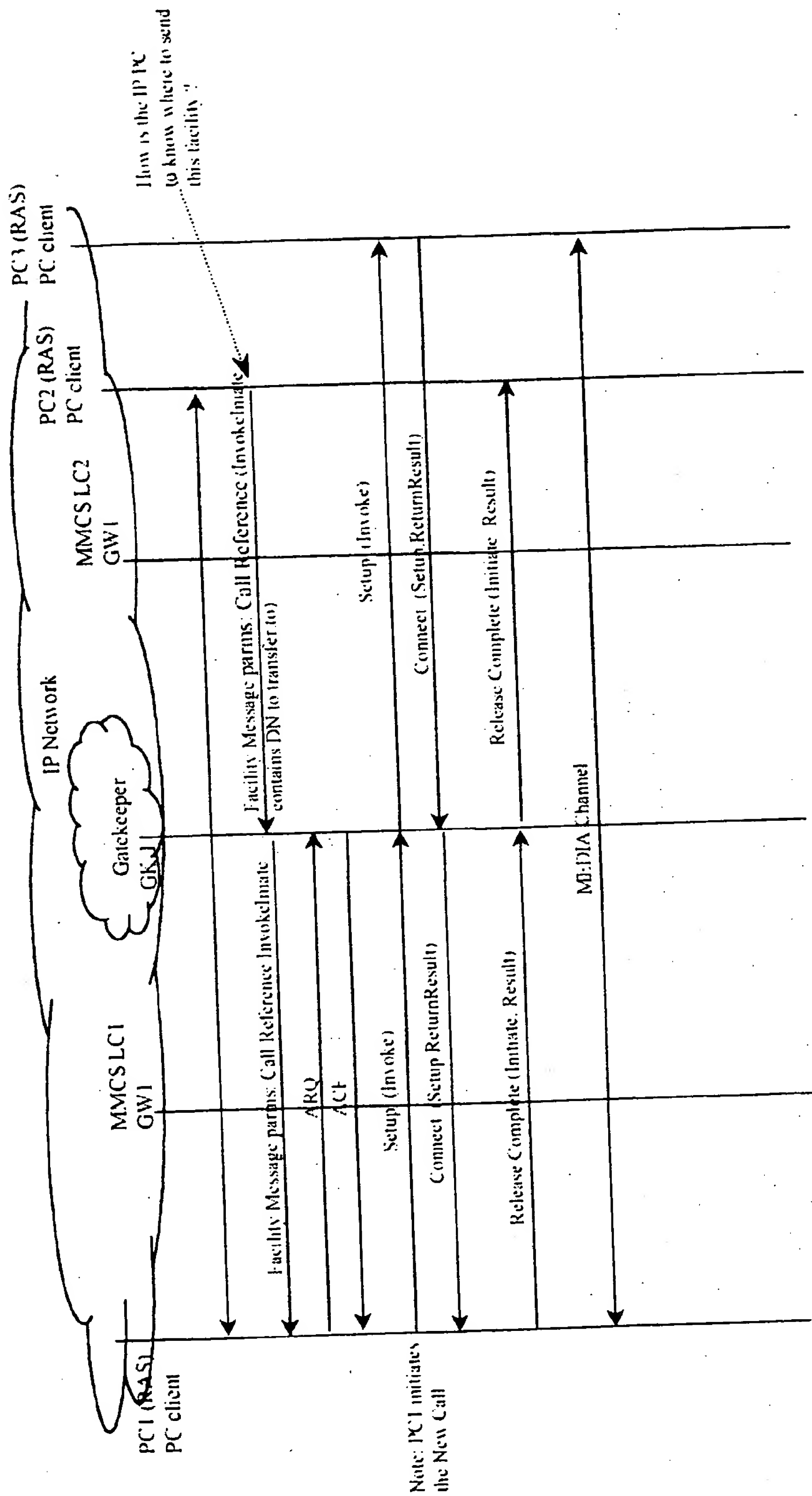
Call Forward & Call Transfer scenarios

APDU Supplementary Services

For Supplementary services:
Q931/H225 Facility IE is set to 00011100 and length 0. All Supplementary services as done in the UUIE.
In the following examples all the parms indicated in blue font are part of the UUIE and the supplementary services and are passed in Q.931/messages.

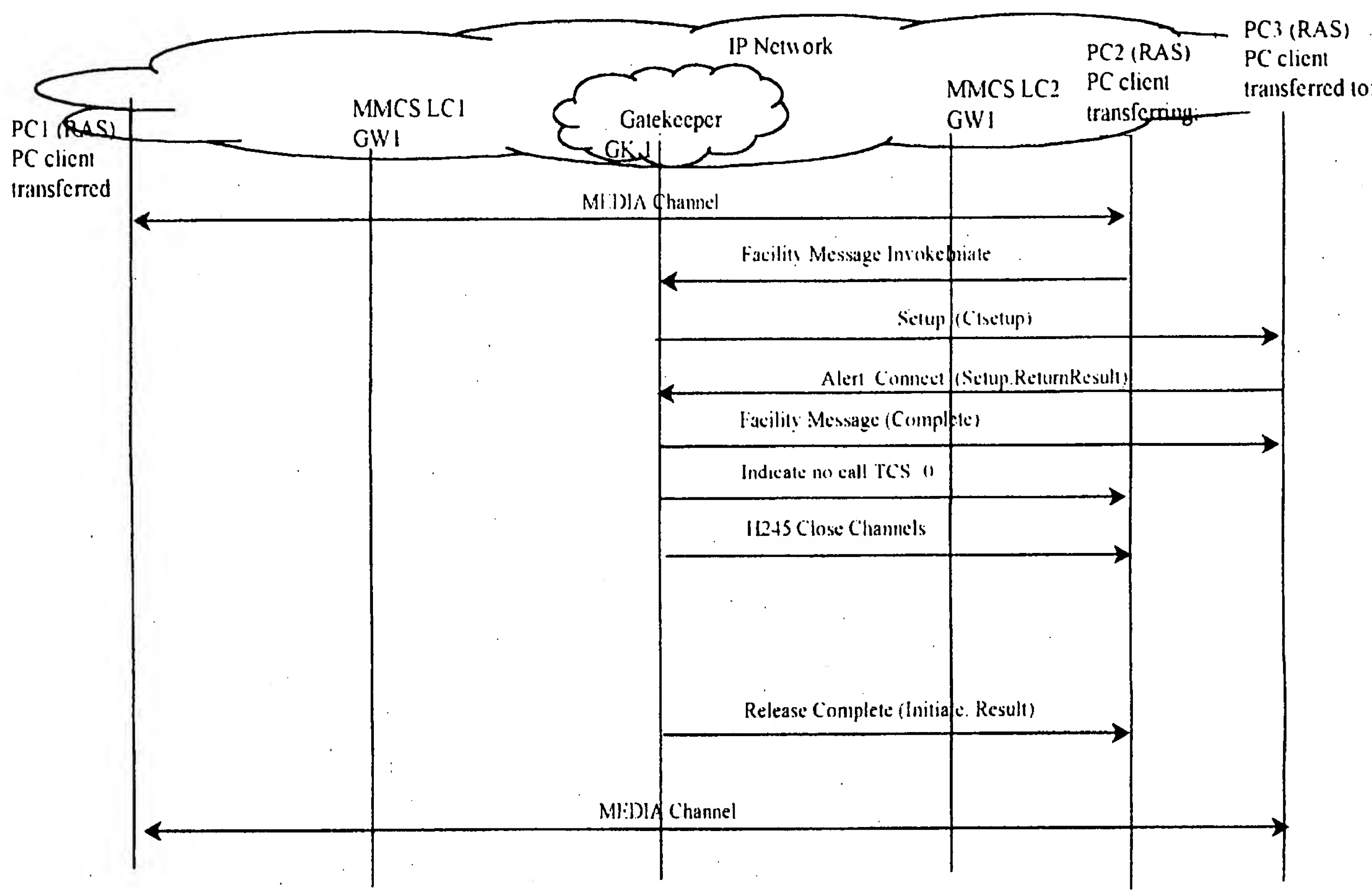
PC2 transfers call to PC3

No Gateway using GK routing - Gatekeeper acts as transparent (H450.2)



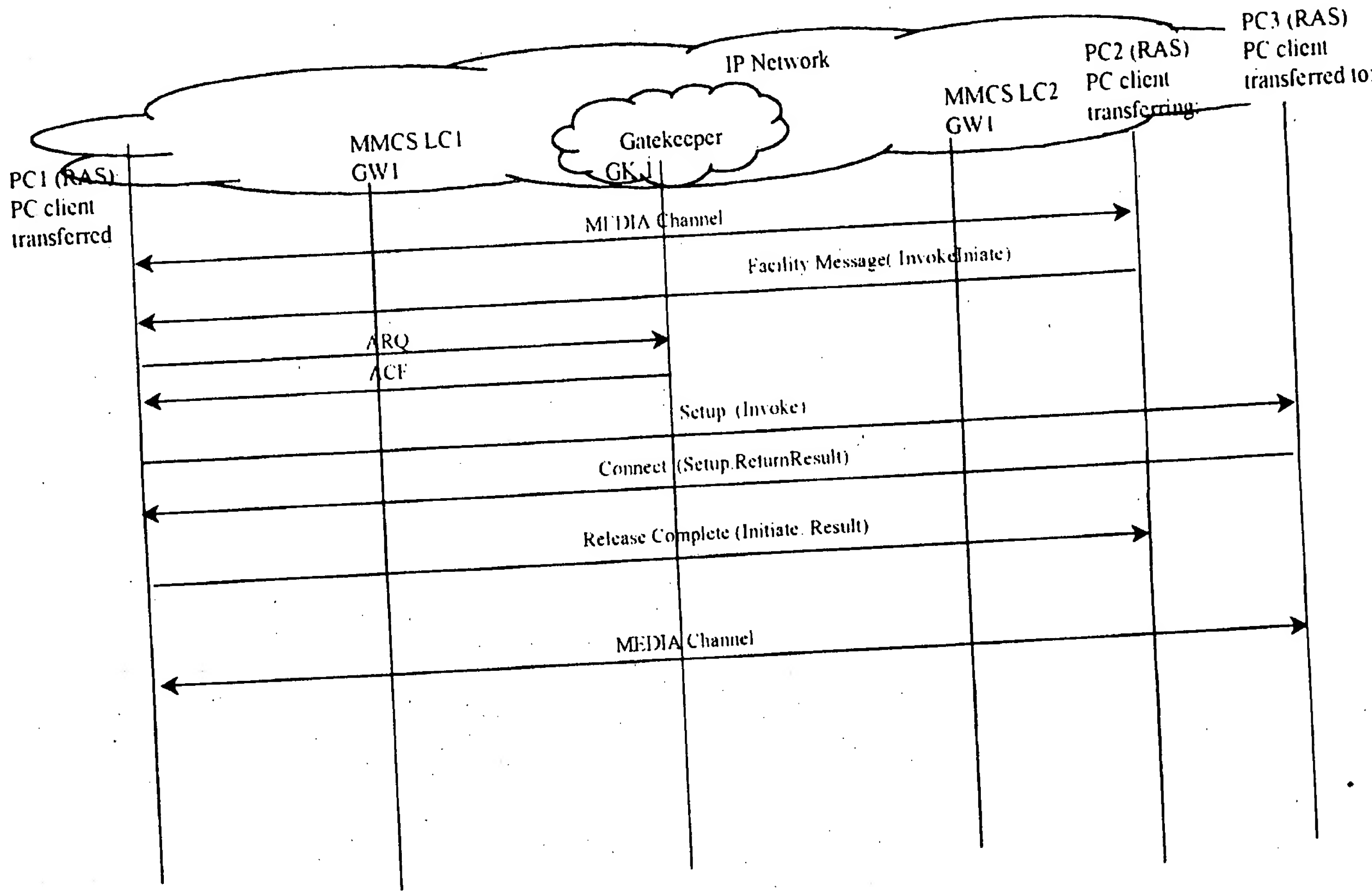
PC2 transfers call to PC3

No Gateway using GK routing - Gatekeeper intercepts APDUs



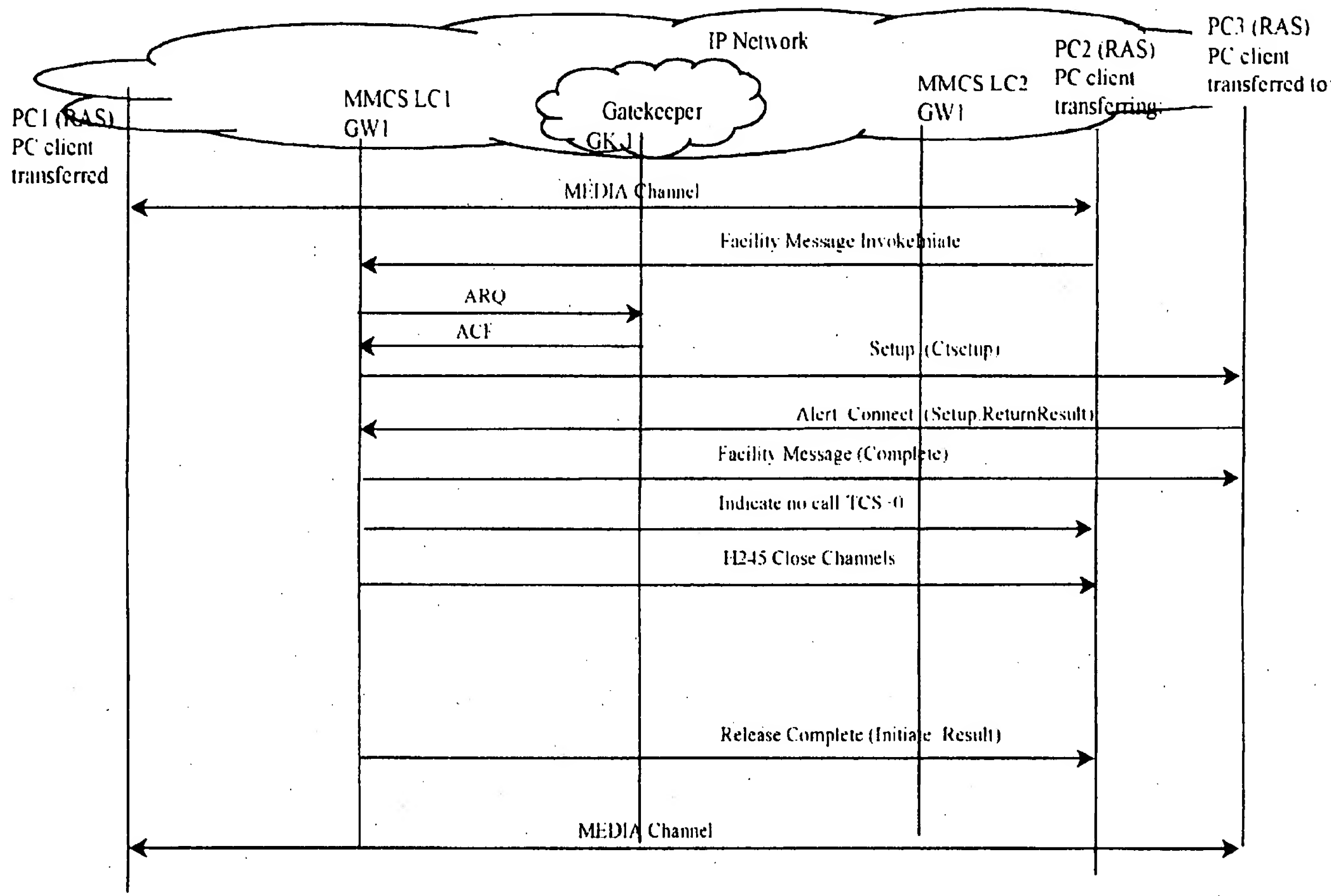
PC2 transfers call to PC3

No Gateway or GK - IP terminal to IP terminal (H450.2)

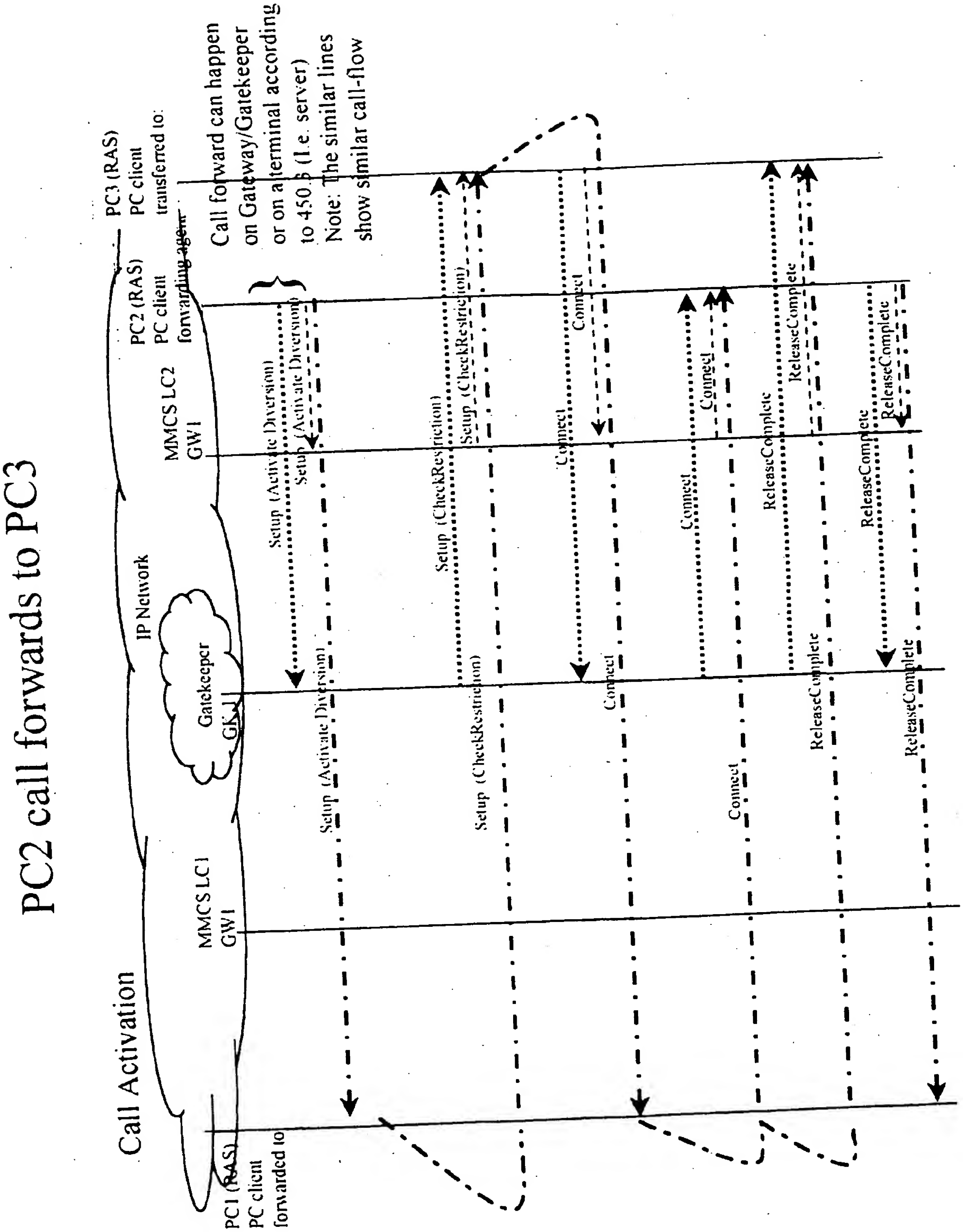


PC2 transfers call to PC3

Gateway intercepts APDUs

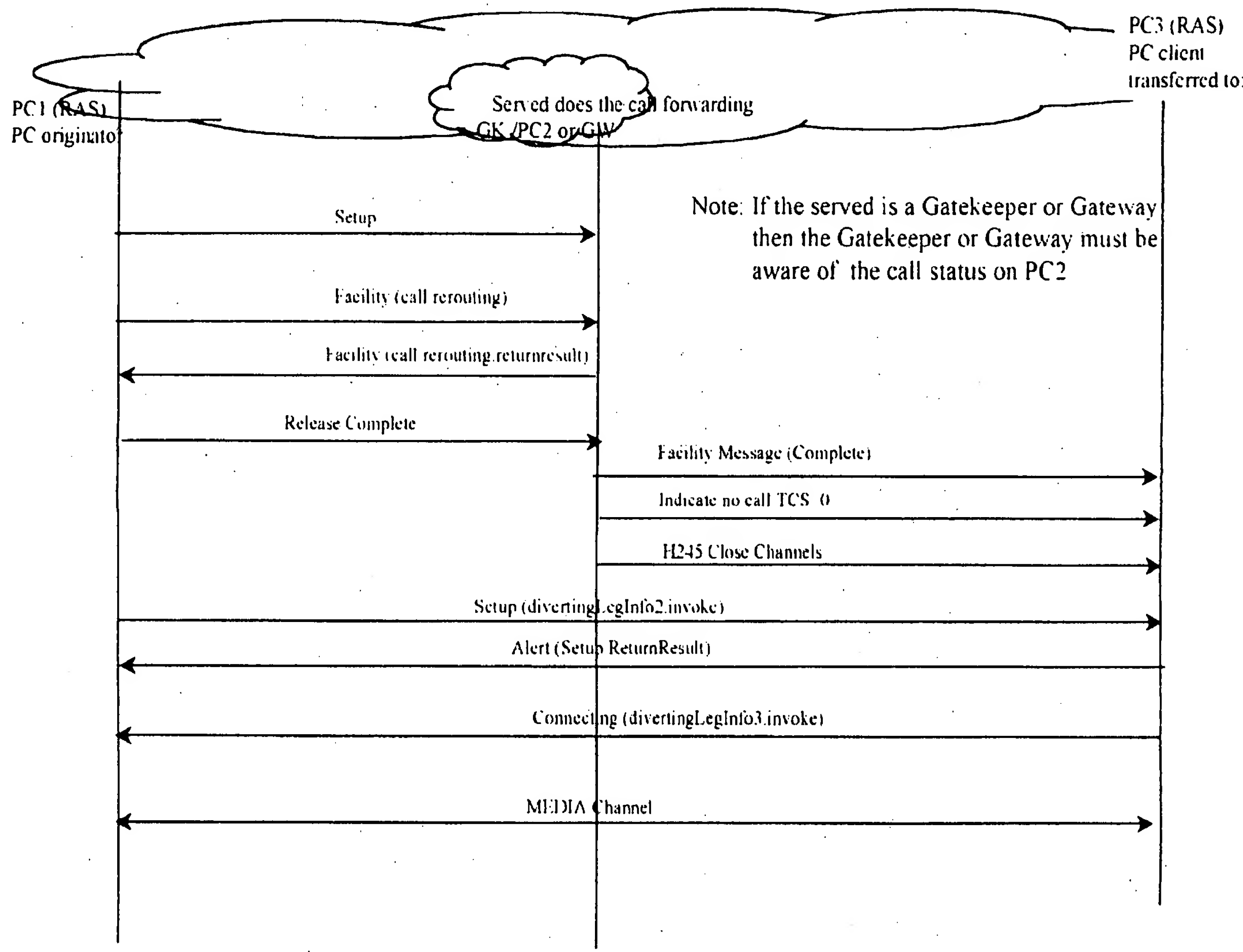


Note: Release complete is not set to the transferring agent until setup to transferred agent is complete


PC2 call forwards to PC3
Call Activation
PC1 (RAS) PC client forwarded to
MMCS LC1 GW1
IP Network
Gatekeeper GK1
MMCS LC2 GW1
PC2 (RAS) PC client forwarding agent
PC3 (RAS) PC client transferred to:
Call forward can happen on Gateway/Gatekeeper or on a terminal according to 450.3 (I.e. server)
Note: The similar lines show similar call-flow
Setup (Activate Diversion)
Setup (CheckRestriction)
Connect
ReleaseComplete

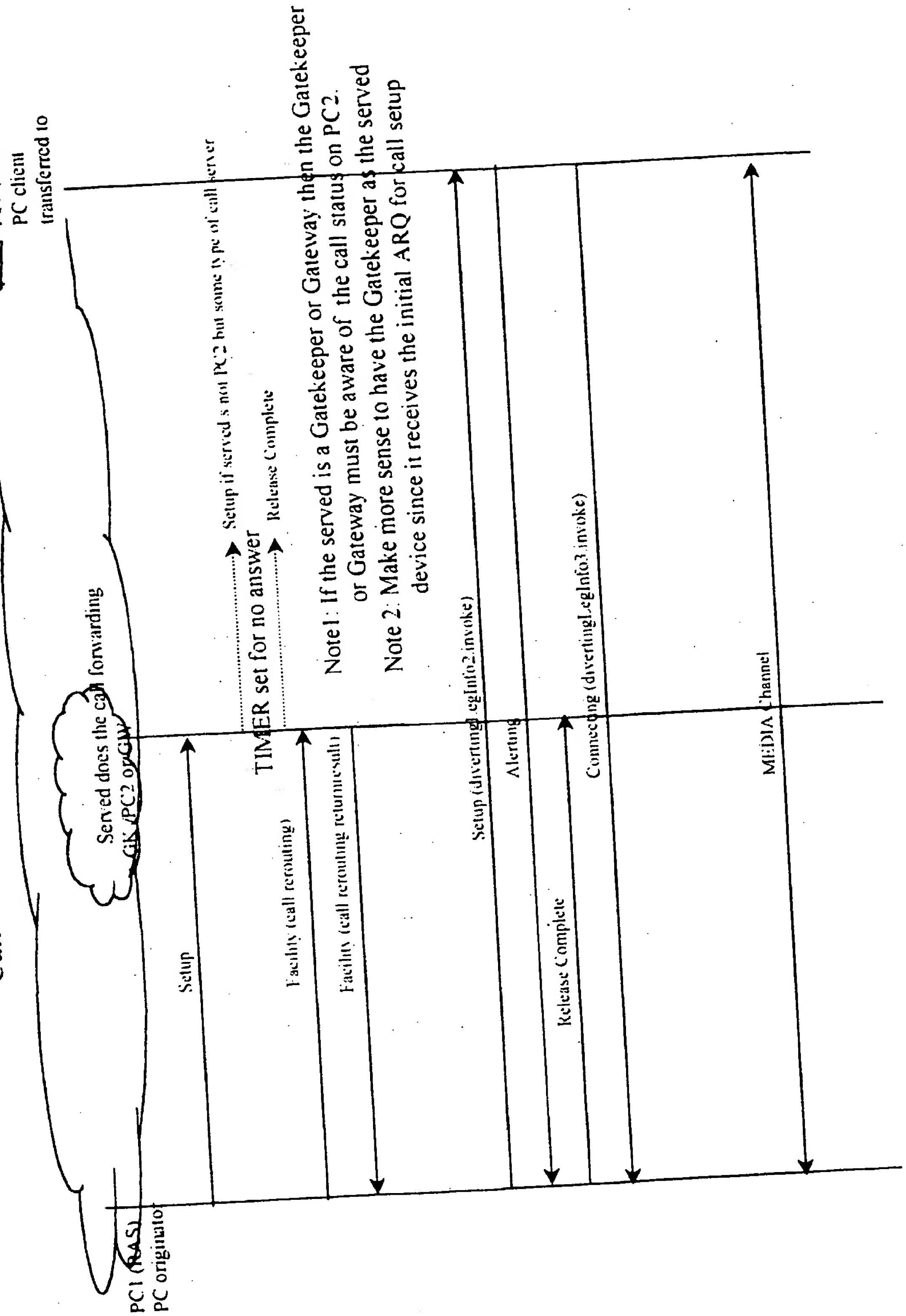
CFU/CFB/CF not registered

Call Forward PC2 to PC3 - CFU/CFB/CF not registered



CF No Answer

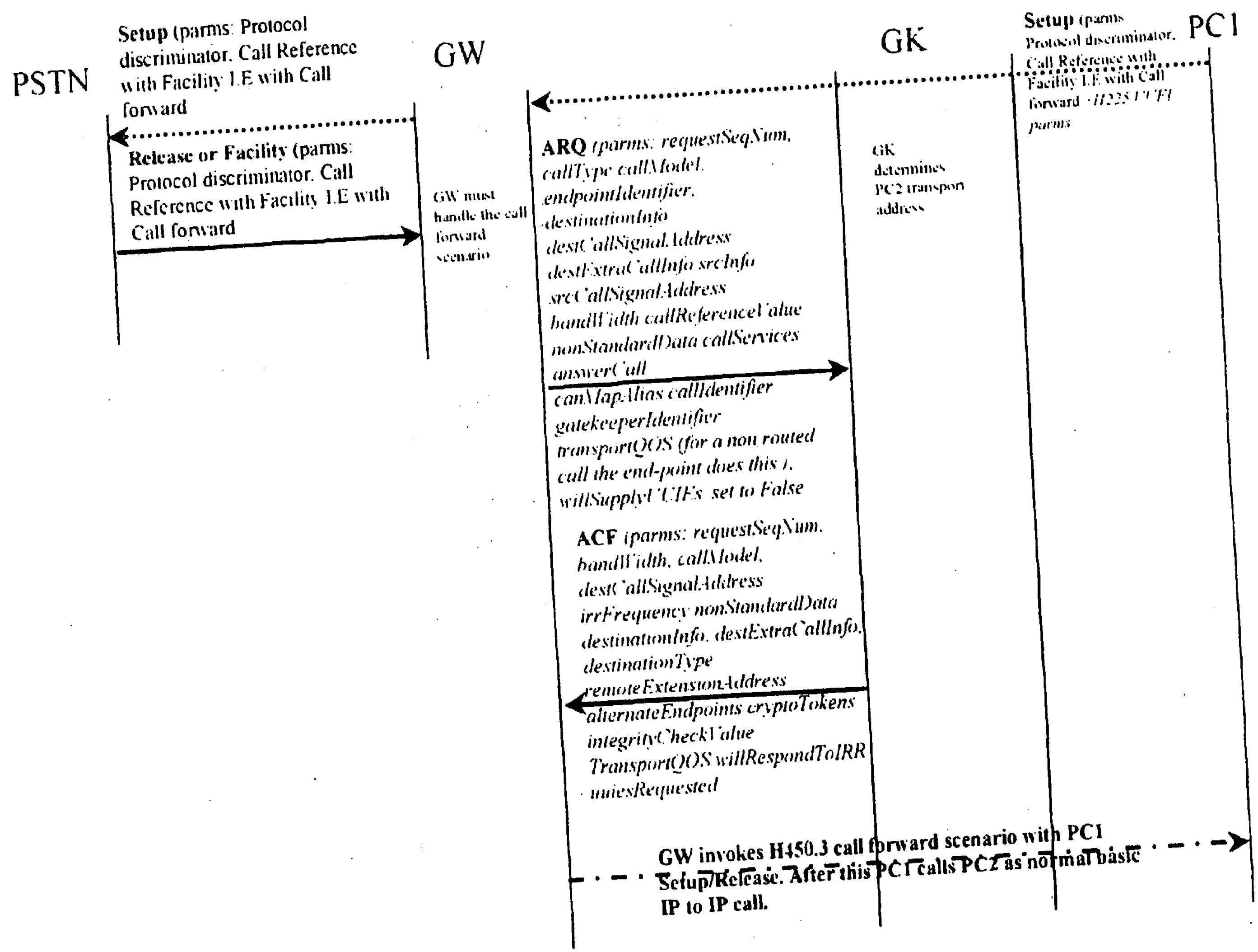
Call Forward PC2 to PC3 - CF No Answer



Call Forward Problems

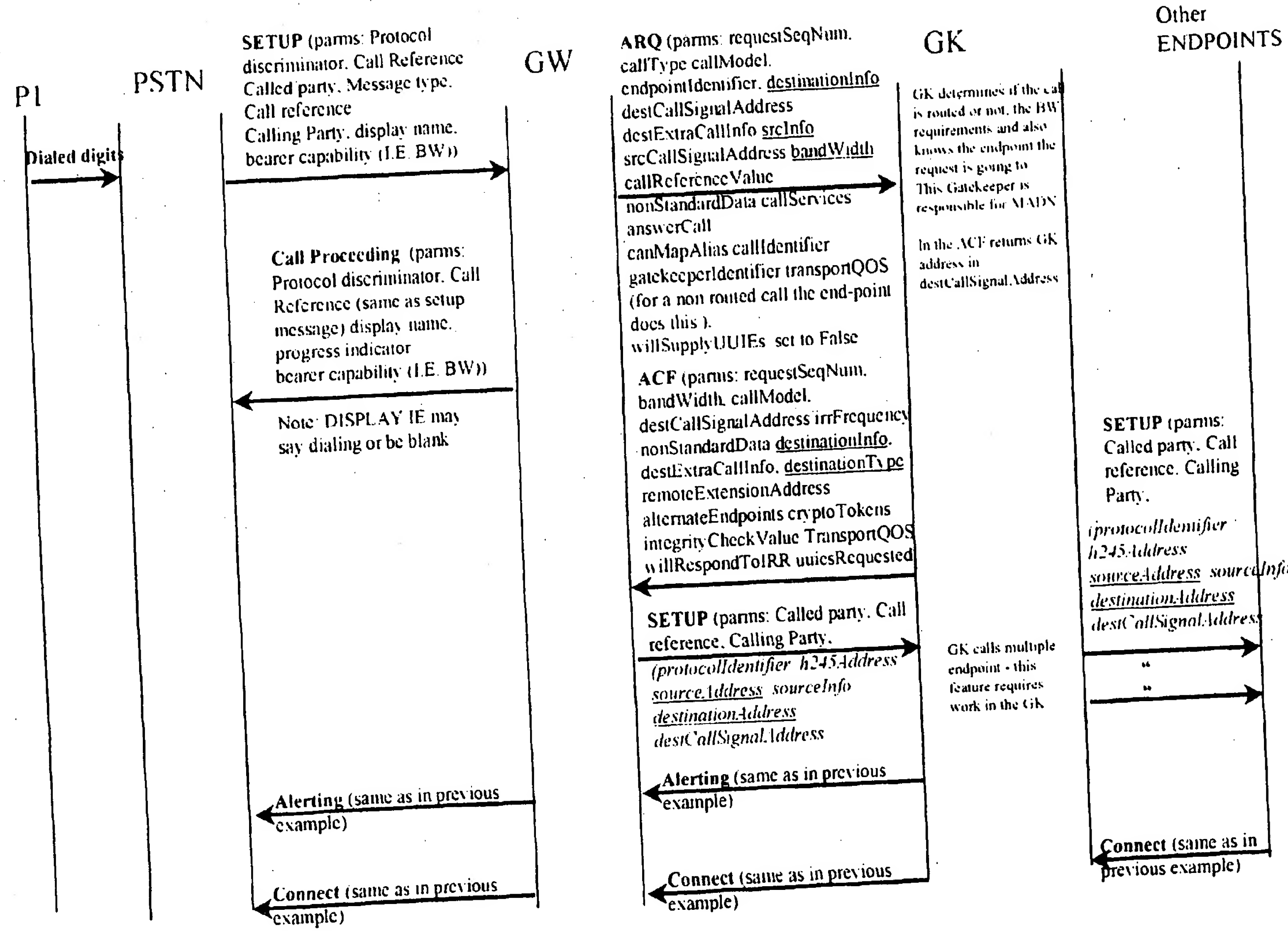
If the originating terminal calls the PC1 (PC1 itself is responsible for call forwarding - SERVED) PC1 is registered but is not responding to setup messaging and hence will not forward the call. It is better to have the SERVED as the GK and possibly the Gateway. Since ARQ call queries are sent to the GK, it is logical to have the call forwarding functionality there also.

PC1 calls P1 which is forwarded to PC2



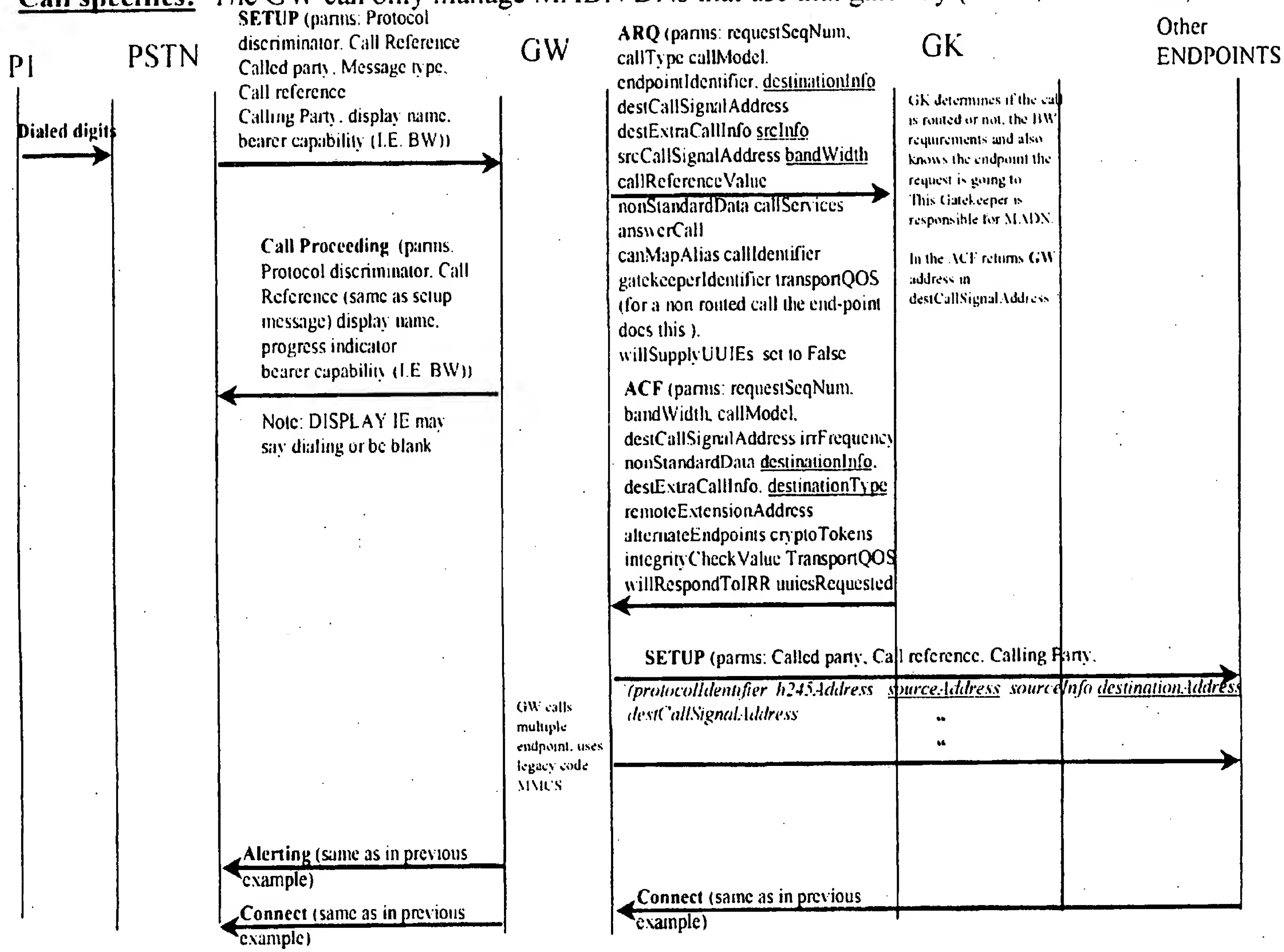
MLA & MADN

MADN: P1 calls a MADN - GK is responsible for MADN



MADN: P1 calls a MADN - GW is responsible for MADN

Call specifics: The GW can only manage MADN DNs that use that gateway (not network-wide)



MLA: P1 calls a MLA PC1 - GK or GW handles

For MLA the Call Scenario is identical to the MADN scenarios for the GK and GW since these devices will handle the call setup. The media channel will be establish after the call has been established and will be direct. The MMCS GW contains legacy code to do but will require modification, however for both the MADN and the MLA services managed by the Gateway, the features are restricted to those terminals served by this Gateway. The gatekeeper would need work for this feature to added.

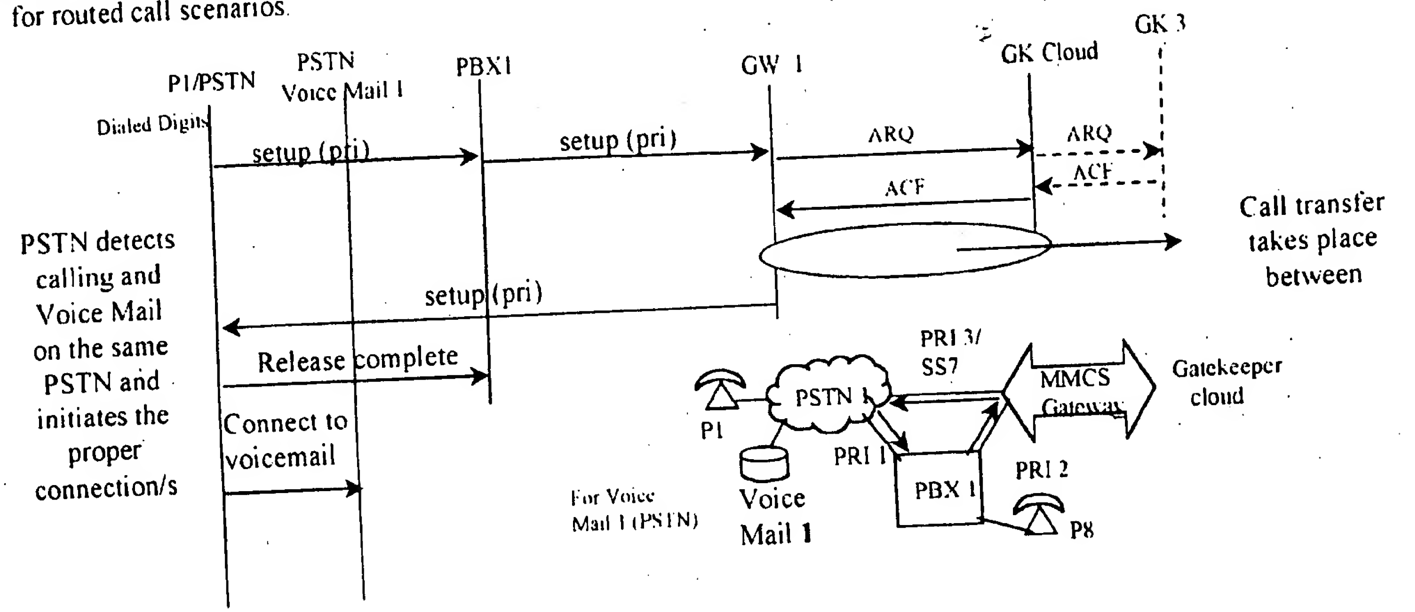
Both MADN and MLA do not require **APDU supplementary services** to be developed as these are features more capably handled by a **Call Server** device, I.E. GW or GK.

Voice Mail Call Flows

P1 to P8 (voice mail on PSTN)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to PC1 which is not registered. Voice Mail 1 on PSTN. Gatekeeper provisioned for WITH voice mail on the gatekeeper for P8. Gatekeeper uses H450.3 to reroute call to Voice Mail1. This only applies for routed call scenarios.



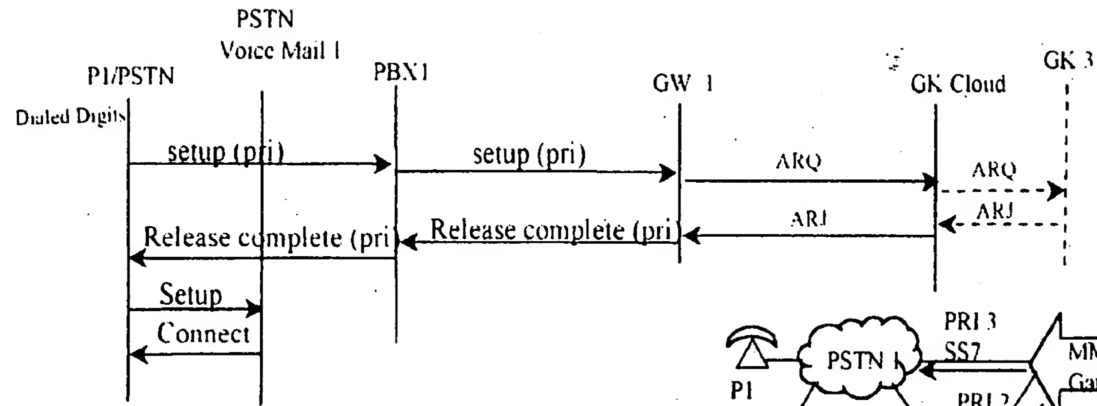
0 DS0's used as PSTN detects P1 and Voice mail on the same PSTN.

- Depending on the setup of the voice mail the callee may be required to enter the number of the phone of the called party, this is NOT desired functionality.

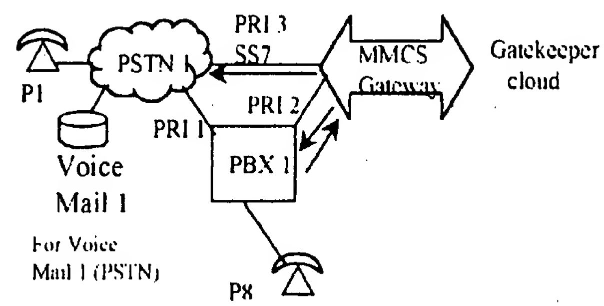
P1 to P8 (voice mail on PSTN)

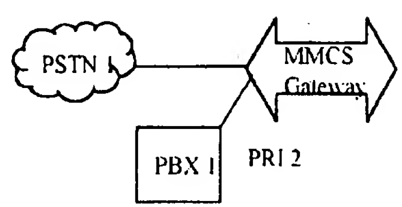
Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not registered**. Voice Mail 1 on PSTN . Gatekeeper rejects call. The PSTN knows that call cannot be terminated because of a release complete message, then the PSTN voice mail is to be used for P8.



0 DS0's used as PSTN detects P1 and Voice mail on the same PSTN. This would work the same way with a call busy scenario (except for the extra setup messages to terminating phone).

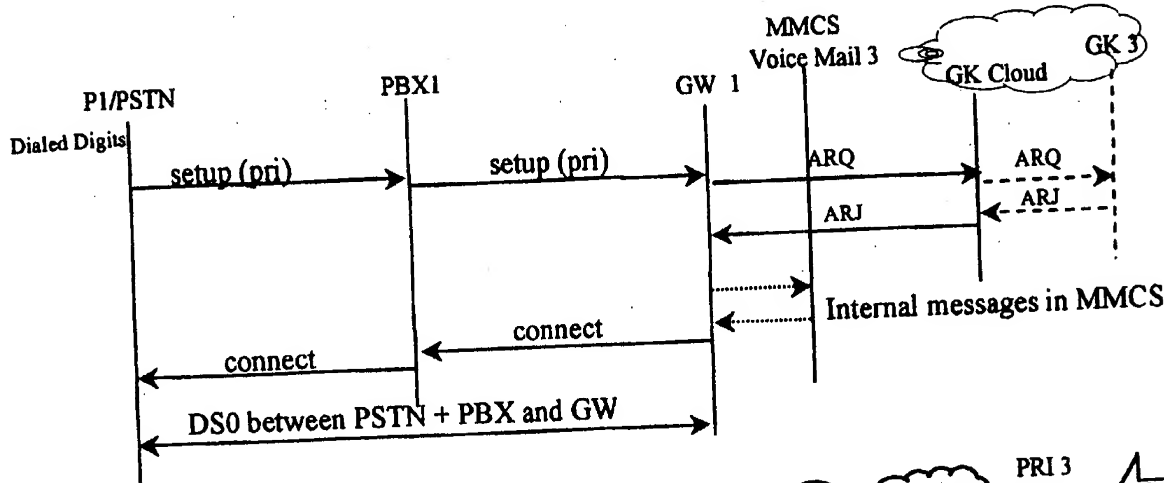




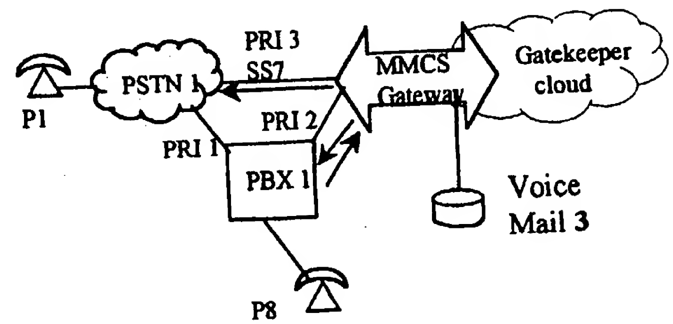
Another option is to have the PBX is connected to MMCS directly. This would cause extra Q9.31 setup messages since all PBX messages will go through the MMCS. **NOT GOOD !!**

P1 to P8 (voice mail on MMCS/GW)

Call specifics.
Call from P1 to P8 (phone on PBX1). P8 is call forwarded to PC1 which is **not registered**. Voice Mail 3 on MMCS/GW.



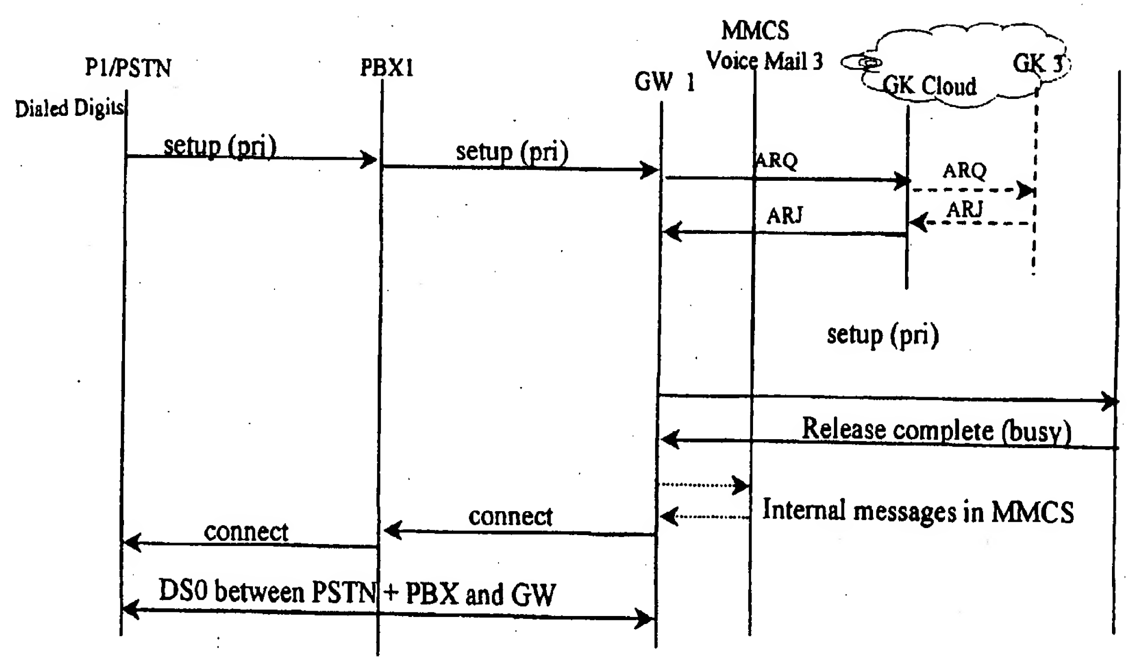
2 DS0's between PSTN and MMCS.



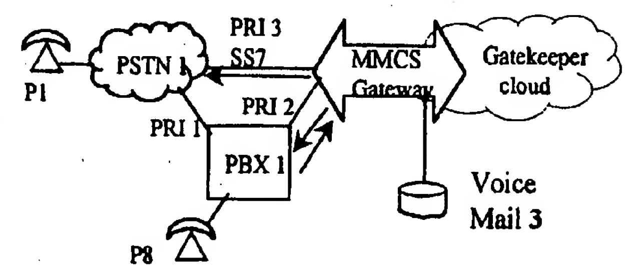
P1 to P8 (voice mail on MMCS/GW)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to a **BUSY PC1**. Voice Mail 3 on MMCS/GW .



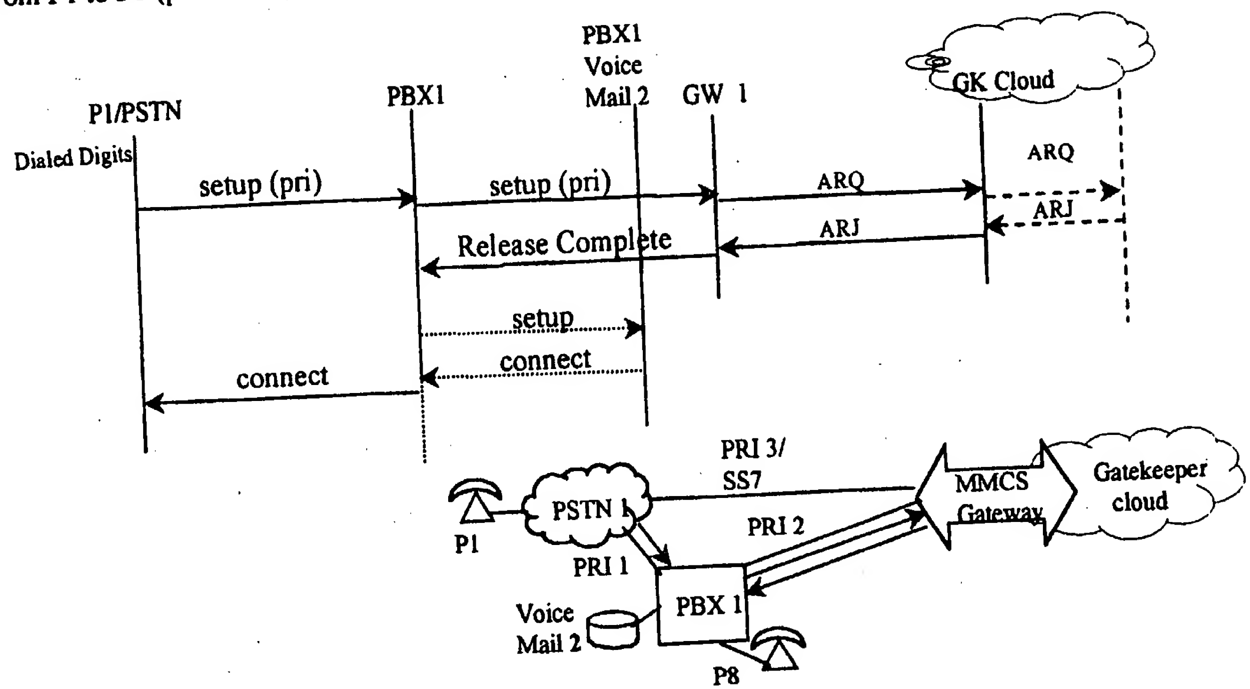
2 DS0's between PSTN and MMCS.



P1 to P8 (voice mail on PBX1 - express mail)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not registered**. Voice Mail **2** on PBX1.

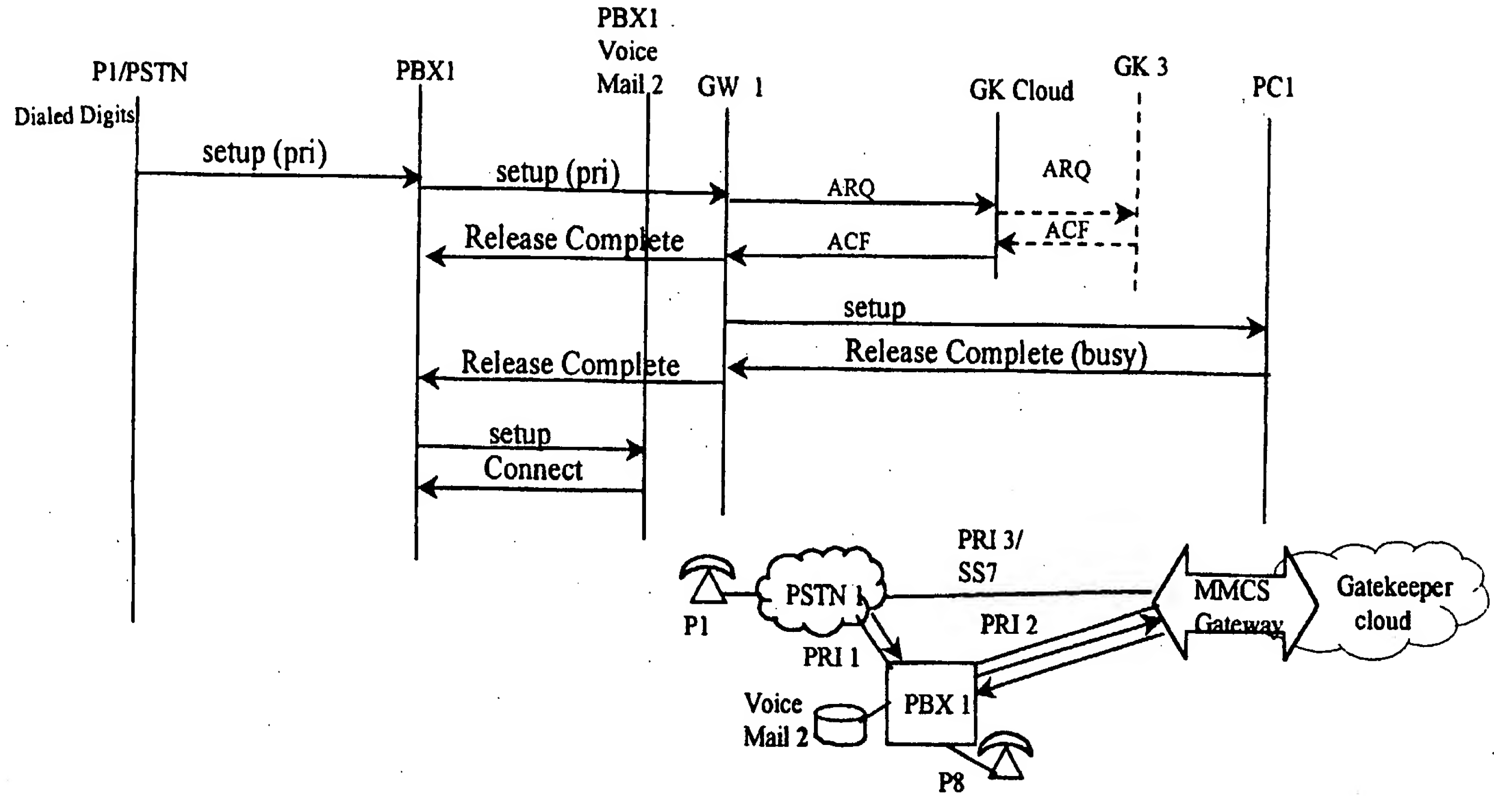


1 DS0 is taken by the call between P1 and Voice Mail 2.
Can the PBX handle a release complete and forward to a internal mail? I Don't believe so!

P1 to P8 (voice mail on PBX1 - express mail)

Call specifics.

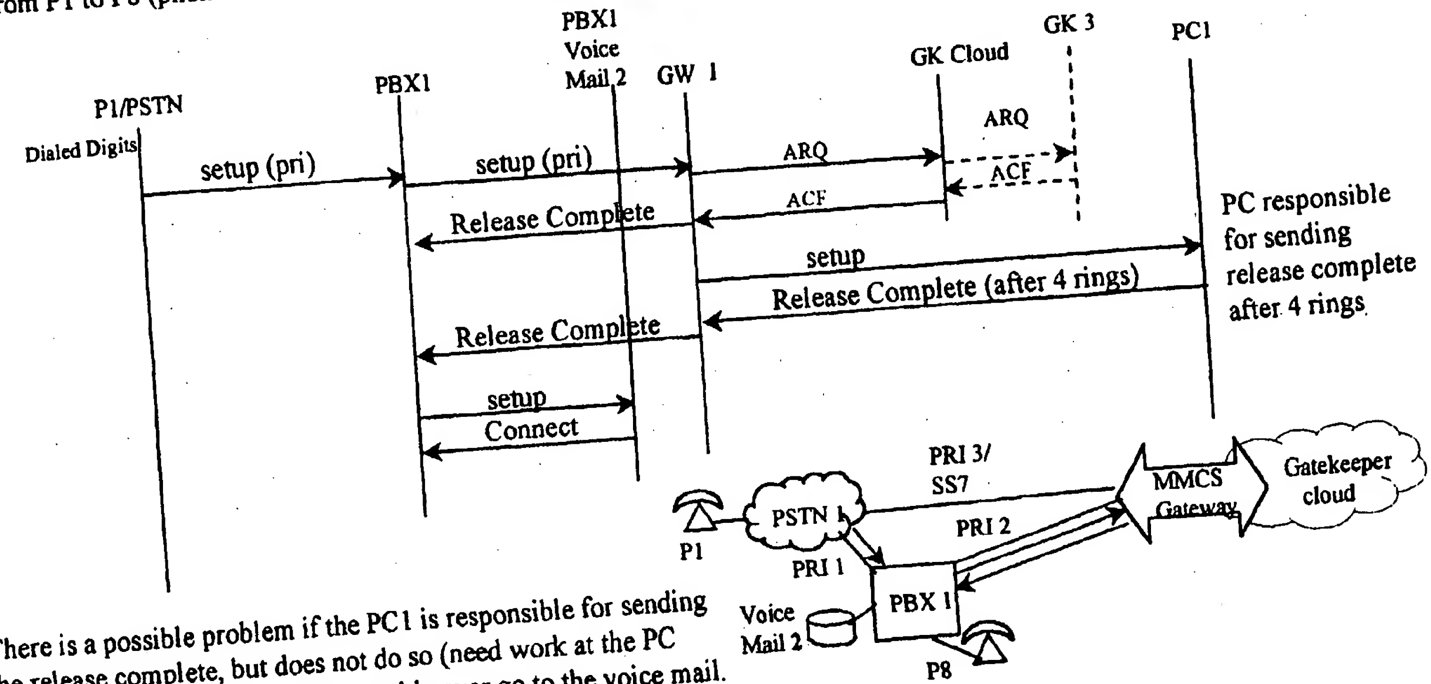
Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is BUSY**. Voice Mail 2 on PBX1.



P1 to P8 (voice mail on PBX1 - express mail)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 but does not answer the phone**. Voice Mail 2 on PBX1.



There is a possible problem if the PC1 is responsible for sending the release complete, but does not do so (need work at the PC client so that after 4 rings). Call would never go to the voice mail. There are 2 other options which illustrated on the following 2 pages:

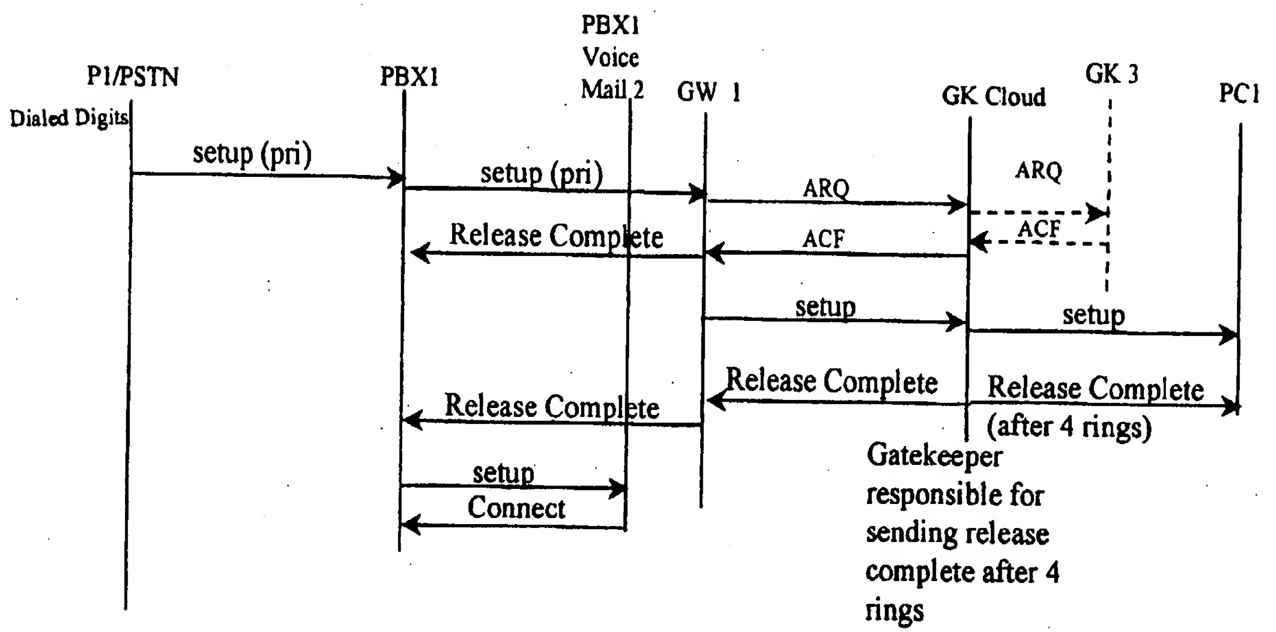
- It may be better to use a routed call model in this case via gatekeeper - Option 1
- After 4 rings the PBXsends a release complete to the gateway and connects to the PBX voice mail. Can the PBX do this presently? - Option 2

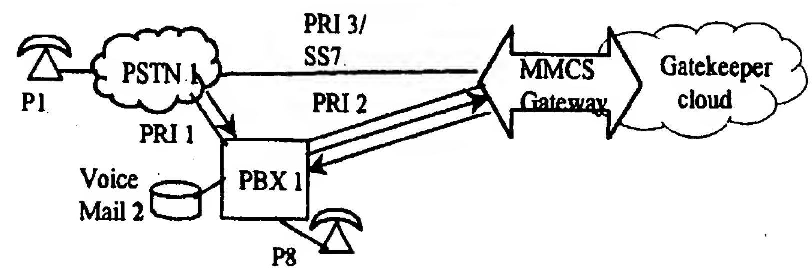
P1 to P8 (voice mail on PBX1 - express mail)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not answering**. Voice Mail 2 on PBX1.

OPTION1: Gatekeeper handles call control (this only works for routed calls)

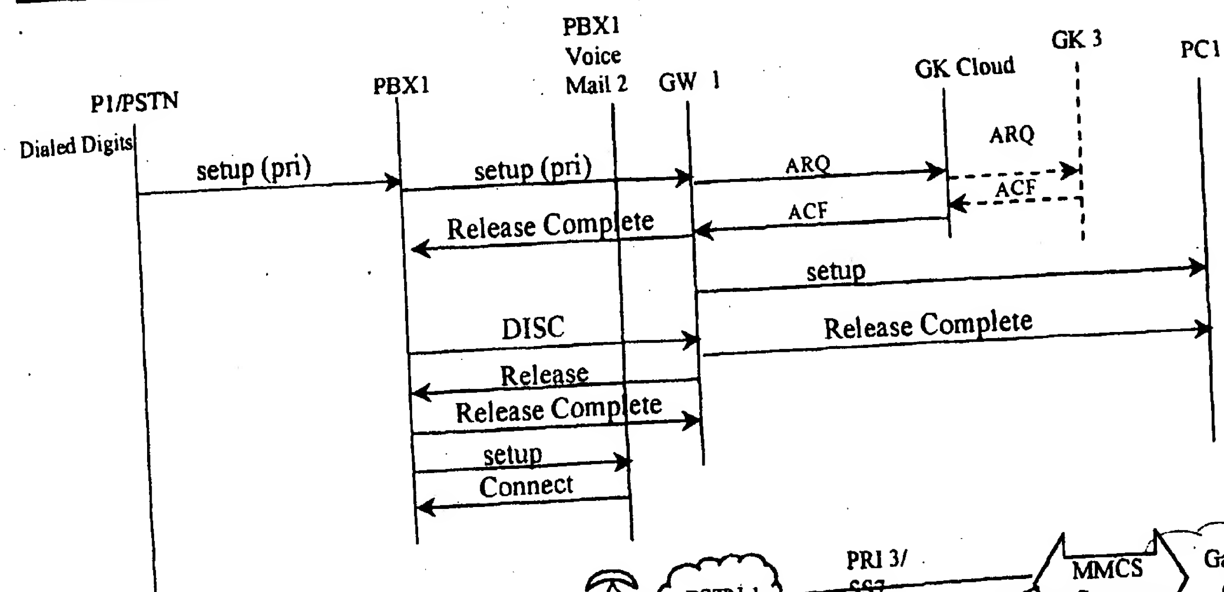


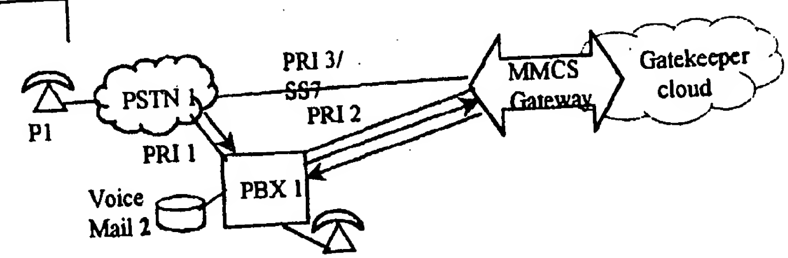


P1 to P8 (voice mail on PBX1 - express mail)

Call specifics.
Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not answering**. Voice Mail 2 on PBX1.

OPTION2: PBX call times out a sends DISCONNECT



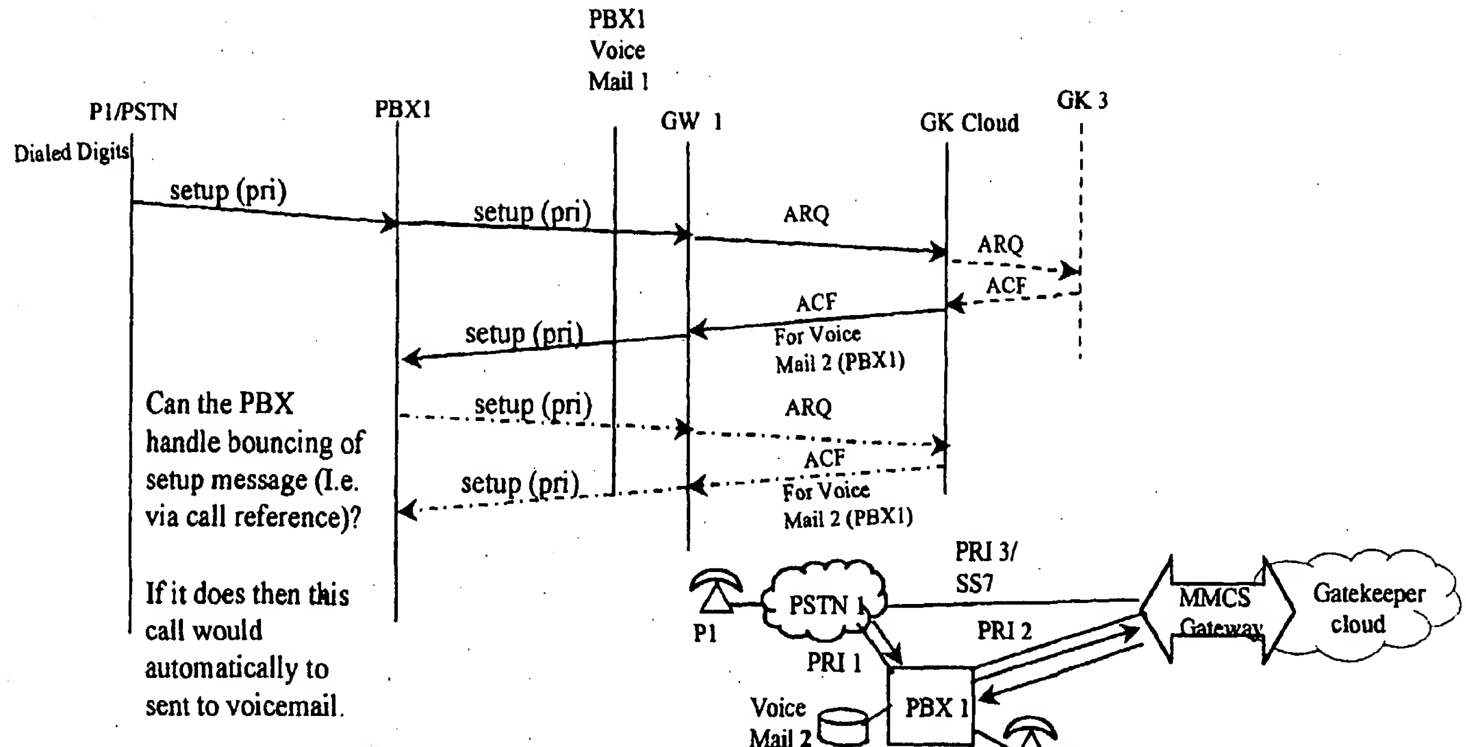


P8

Scenario B: P1 to P8 (voice mail on PBX1 - return call to DN on P8)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not registered**. If the PC1 cannot be reached so the gatekeeper is provisioned to to send calls sent to the DN on P8. Essentially this equivalent to P8 and PC1 forwarded to each other and the setup messages could potentially bounce until CP resources are exhausted unless detected (Need to put this in a testcase)

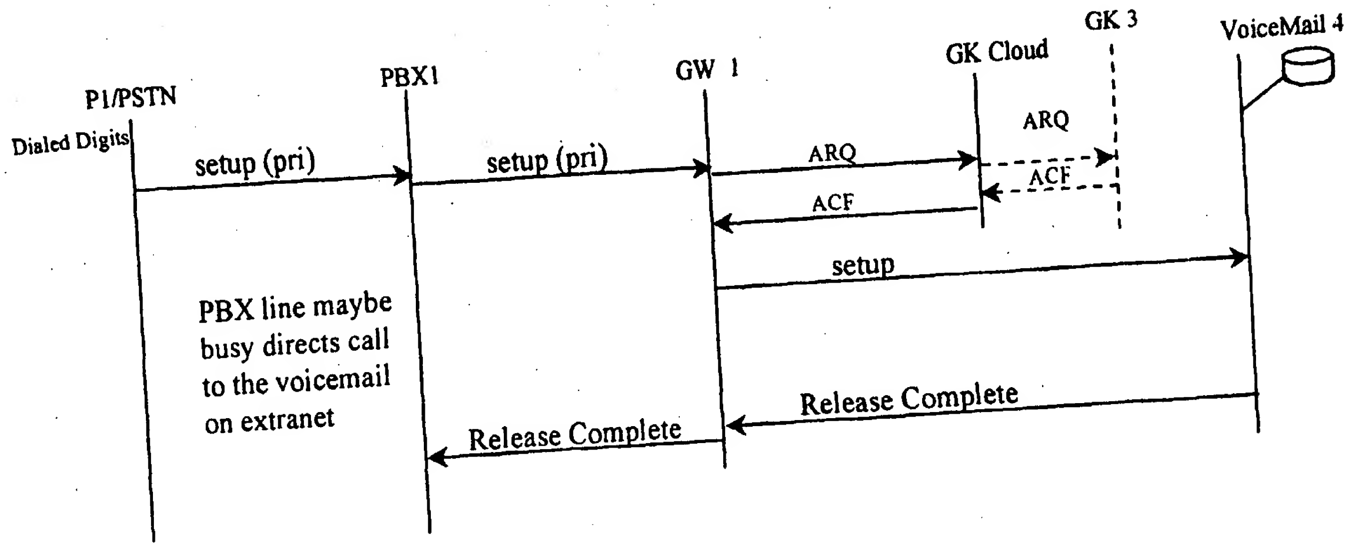


This call takes up 3 trunks (I.E. 3 DS0's).

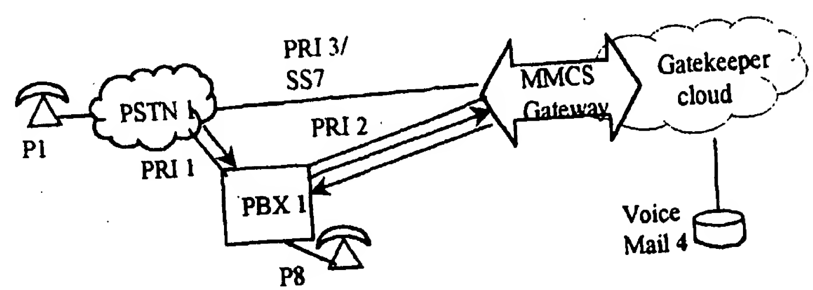
- Depending on the setup of the voice mail the callee may be required to enter the number of the phone of the called party, again as in the last scenario this is not desired functionality as they maybe required to enter the 5digit corporate DN instead of the E.164 dialled (ambiguous DN).

P1 to P8 (voice mail on Extranet)

Call specifics.
Call from P1 to P8 (phone on PBX1). Voice Mail 4 on extranet.



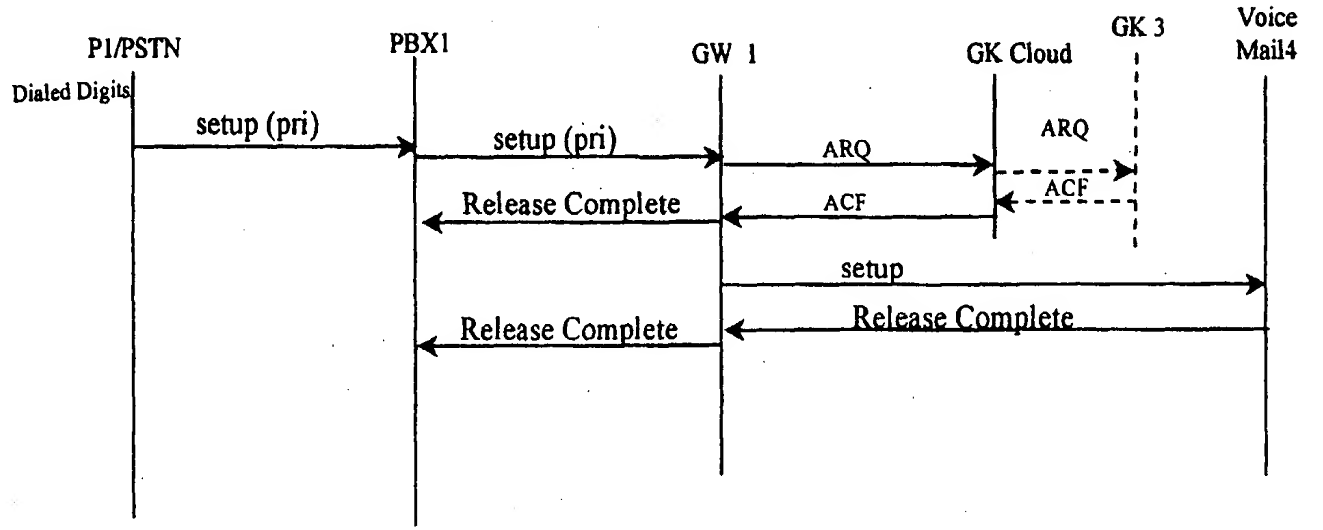
Gatekeeper routes call to VoiceMail 4



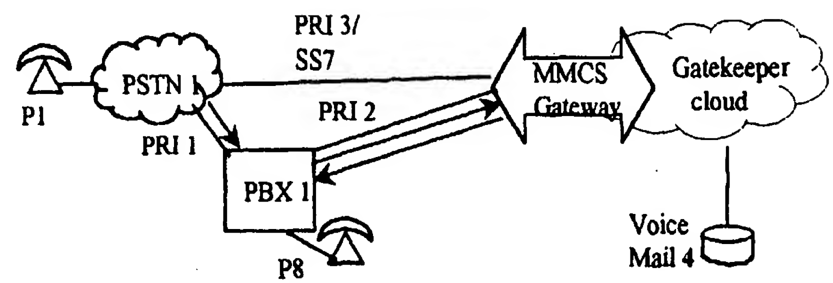
P1 to P8 (voice mail on Extranet)

Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is not registered**. Voice Mail 4 on extranet



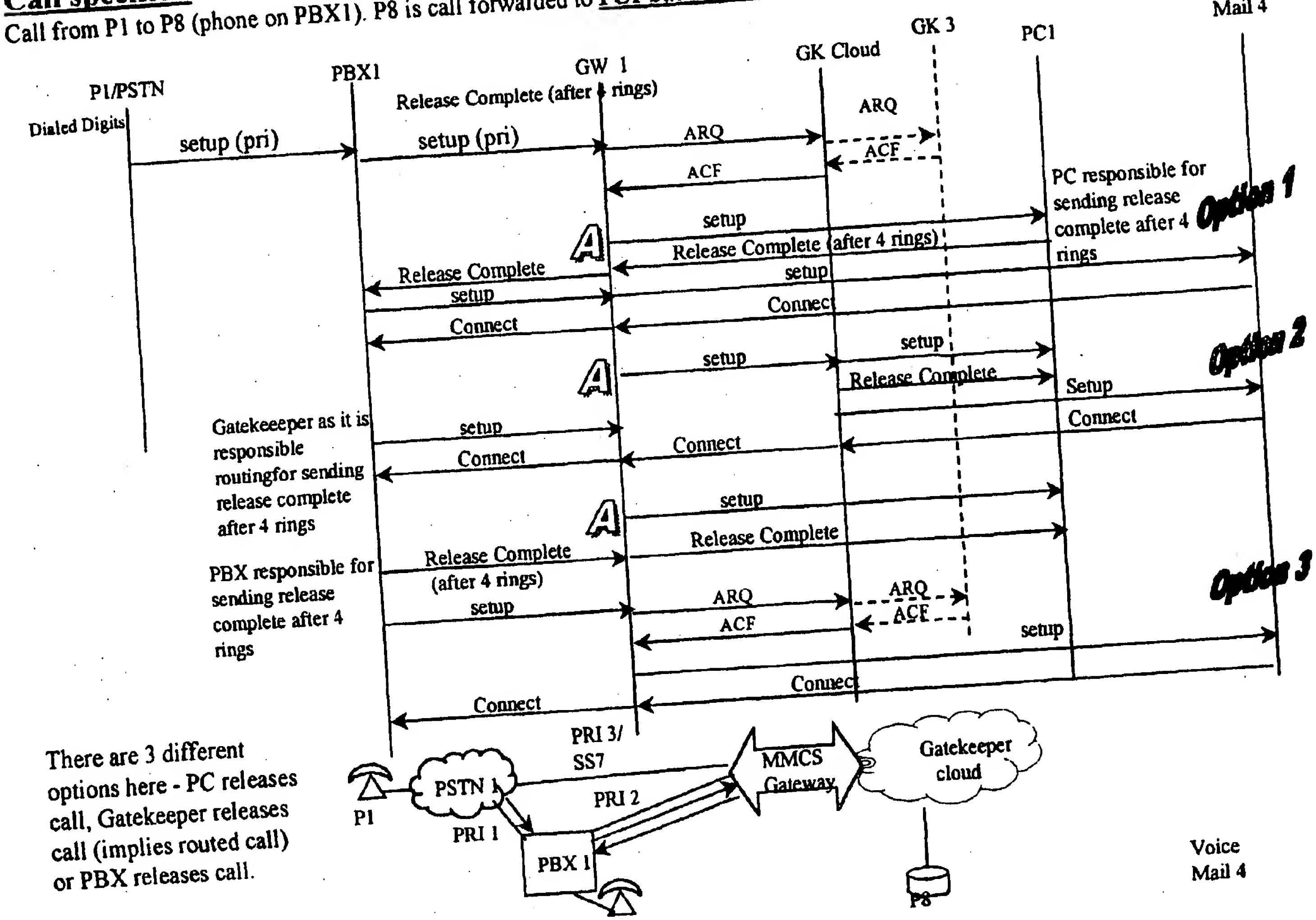
Gatekeeper routes call to VoiceMail 4



P1 to P8 (voice mail on Extranet)

Call specifics.

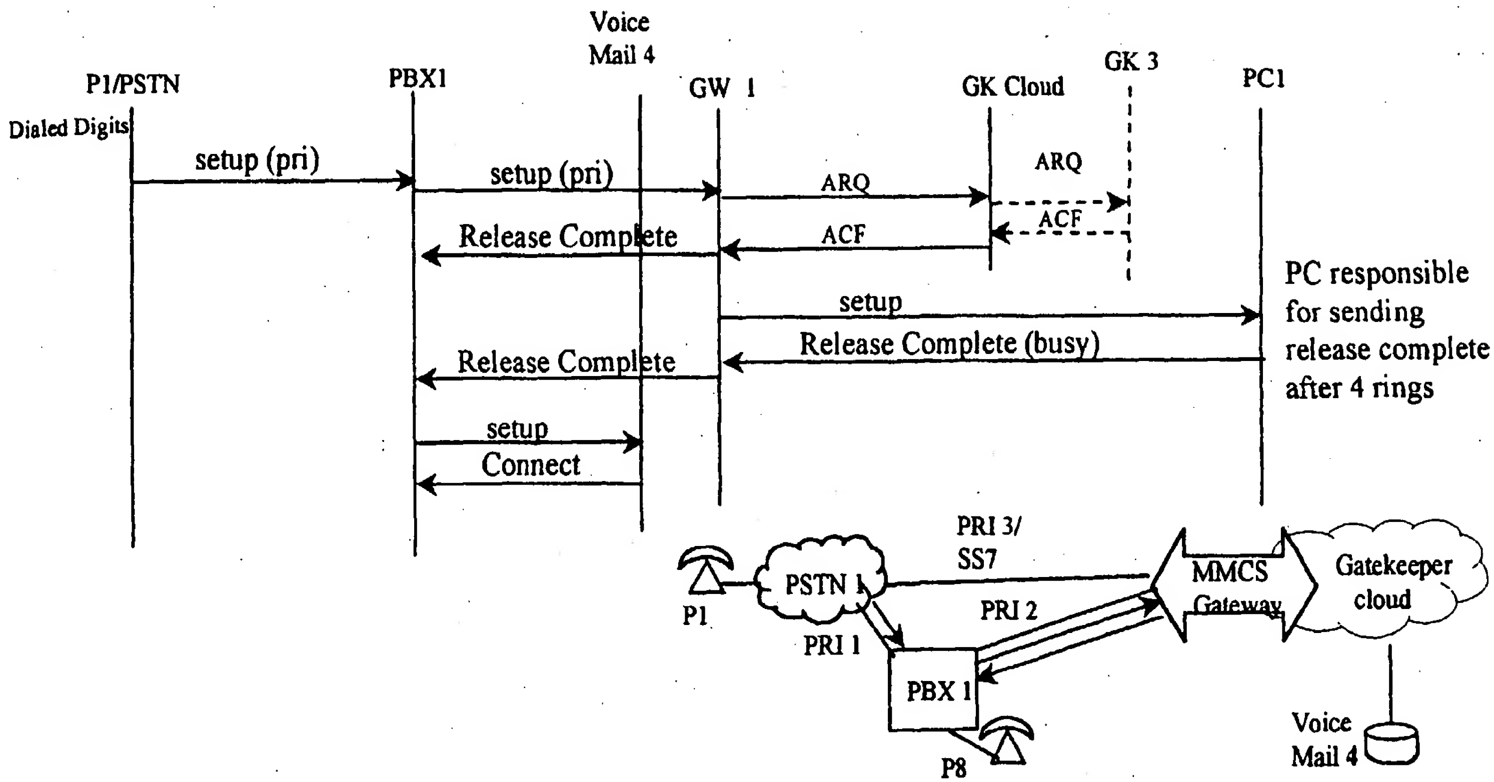
Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 but does not answer the phone**. Voice Mail 4 on Extranet.



P1 to P8 (voice mail on Extranet)

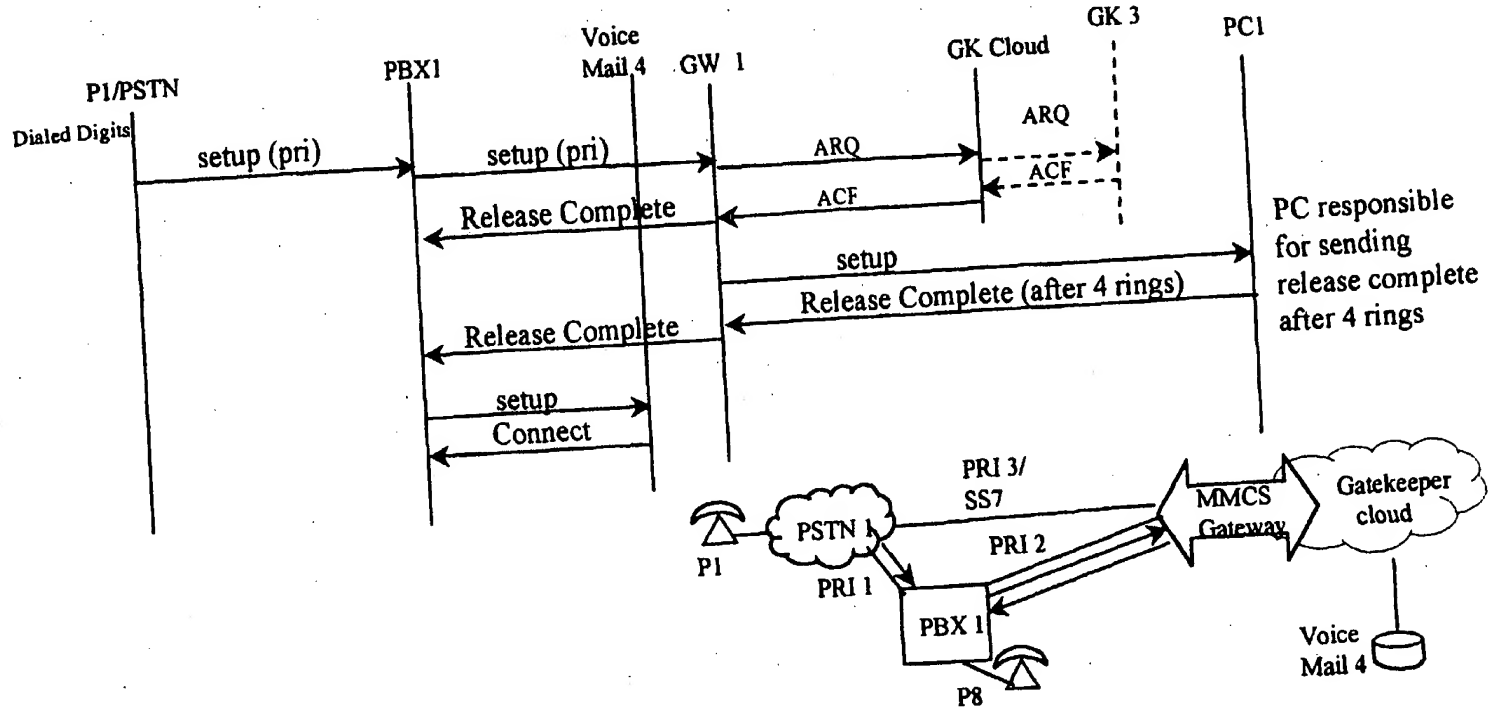
Call specifics.

Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **PC1 which is busy**. Voice Mail 4 on Extranet.



P1 to P8 (voice mail on Extranet)

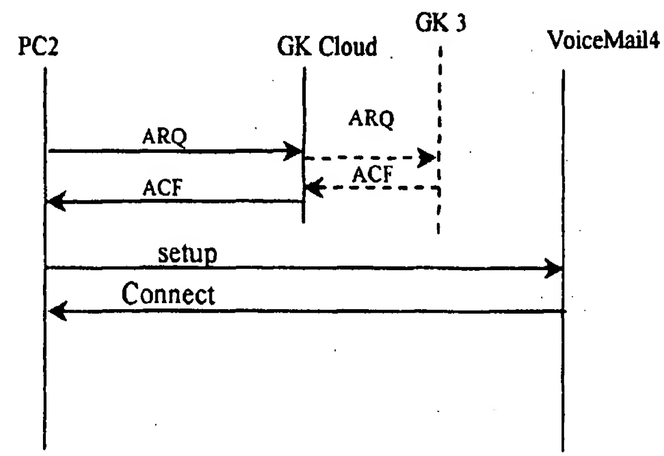
<u>Call specifics.</u>
Call from P1 to P8 (phone on PBX1). P8 is call forwarded to **<u>PC1 but does not answer the phone</u>**. <u>Voice Mail 4</u> on Extranet.

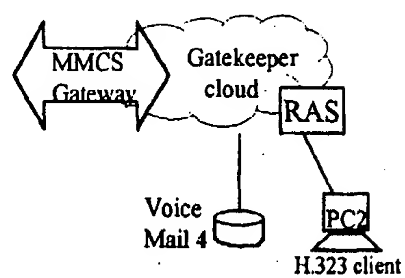


Calling PC1 via gateway or within extranet (voice mail on Extranet)

Call specifics.

Call to PC1but PC1 is not registered. Voice Mail 4 on Extranet.





Calling PC1 via gateway or within extranet (voice mail on Extranet)

Call specifics.

Call to PC1but **PC1 is connected to voiceMail.** Voice Mail 4 on Extranet.

For these scenarios there are 2 options:

1) The gatekeeper could route the call and handles all call processing for call setup and release (I.e. checking if PC1 is not answering or busy then routing call to voice mail4 This requires work in Gatekeeper.

2) Or use the call forwarding scenarios (**CFU/CFB/CF not registered page in slides**). The Served (node responsible for call forwarding, normally a gatekeeper) forward calls to voice mail. This also requires work in gatekeeper or PC client depending which node is the **served.**

IP TELEPHONY GATEWAY APPENDIX 4

Mapping between Q931 parameters and the H225/ARQ parameters

Mapping Q931 parms to H225/ARQ parms

H225/ARQ message	Q.931 on PSTN
requestSeqNum	
callType *use point-to-point default*	
callModel. *Direct or gatekeeper routed*	
endpointIdentifier *GW,GK or terminal* .	
destinationInfo *E.164 called number*	**called party**
destCallSignalAddress *transport address used at the destination for call signaling.*	
destExtraCallInfo	
srcInfo *E.164 calling number*	**calling party**
srcCallSignalAddress - *transport address used at the source for call signaling.*	**bearercapability**
bandWidth - *the number of 100 bps requested for the bi-directional call.*	
callReferenceValue - *the CRV from Q.931 for this call; only local validity. This is used by a gatekeeper to associate the ARQ with a particular call.*	**callreference** may be not the same as on the Gateway
nonStandardData - *carries information not defined in this recommendation (for example, proprietary data)*	
callServices - *provides information on support of optional Q-series protocols to gatekeeper and called terminal.*	**3WC call ?** **Conference Call using Multicasting** "
conferenceID - *unique conference identifier.*	
activeMC - *if TRUE, the calling party has an active MC, otherwise FALSE.*	
answerCall - *used to indicate to a gatekeeper that a call is incoming.*	
canMapAlias *TRUE indicates ACF containing destinationInfo, destExtraCallInfo and or remoteExtension fields, can be copied this information to the same fields in SETUP message respectively.*	
callIdentifier *a globally unique call identifier set by the originating endpoint which can be used to associate RAS signaling with the modified Q.931 signaling used in H.225.0*	**Not a Callreference**
srcAlternatives *prioritized source endpoint alternatives for srcInfo,* ***srcCallSignalAddress****, or rasAddress*	**alternative calling party not part of Q.931**
destAlternatives *a sequence of prioritized destination endpoint alternatives for* ***destinationInfo*** *or destCallSignalAddress*	
gatekeeperIdentifier *gatekeeperIdentifier received in the alternateGatekeeper list in RCF*	
integrityCheckValue *encryption requirements*	
transportQOS *indicates QOS reservations done at endpoint, GK or none.*	
willSupplyUUIEs *set to False if the gatekeeoer does not require to see all UUIE call control messages.*	

Mapping Q931 parms to H225/ARQ parms

H225/ACF message | **Q.931 on PSTN**

requestSeqNum - *This shall be the same value that was passed in the ARQ.*

bandWidth - *the allowed maximum bandwidth for the call; may be less than that requested.* → **bearercapability**

callModel - *tells terminal whether call signaling sent on destCallSignalAddress goes to a gatekeeper (routed call) or to a terminal(direct call).*

destCallSignalAddress - *the transport address to which to send Q.931 call signaling, but may be an endpoint or gatekeeper address depending on the call model in use.*

irrFrequency - *the frequency, in seconds, that the endpoint shall send IRRs to the gatekeeper while on a call, including while on hold. If not present, the endpoint does not send IRRs while active on a call, and it is expected that the gatekeeper will poll the endpoint*

nonStandardData - *carries information not defined in this recommendation (for example, proprietary data)*

destinationInfo *the address of the initial channel, used when calling through a gateway*

destExtraCallInfo - *needed to make possible additional channel calls, i.e. for a 2*64 Kbps call on the WAN side. Shall only contain E.164 addresses and shall not contain the number of the initial channel.*

destinationType - *This specifies the type of the destination endpoint i.e. gatekeeper, gateway, mcu, or terminal*

remoteExtensionAddress - *contains the alias address of a called endpoint in cases where this information is needed to traverse multiple Gateways*

alternateEndpoints - *a sequence of prioritized endpoint alternatives destCallSignalAddress or destinationInfo*

tokens - *This is some data which may be required to allow the operation. The data shall be inserted into the message if available.*

cryptoTokens - *encrypted tokens*

integrityCheckValue - *cryptographically based integrity check value*

TransportQOS - *Gatekeeper may indicates to the endpoint responsible for resource reservation.*

willRespondToIRR - *true if the Gatekeeper will send an IACK or INAK message in response to an unsolicited IRR message when the IRR's needsResponse field set to true.*

uuiesRequested *indicates the set of H.225.0 call signaling messages of which the endpoint shall notify the gatekeeper.*

SETUP UUIE message	H.225/Q.931 Setup header	Q.931 from PSTN
sourceAddress →	callingparty IE	callingparty IE
sourceInfo →	calledparty	calledparty

SETUP UUIE message

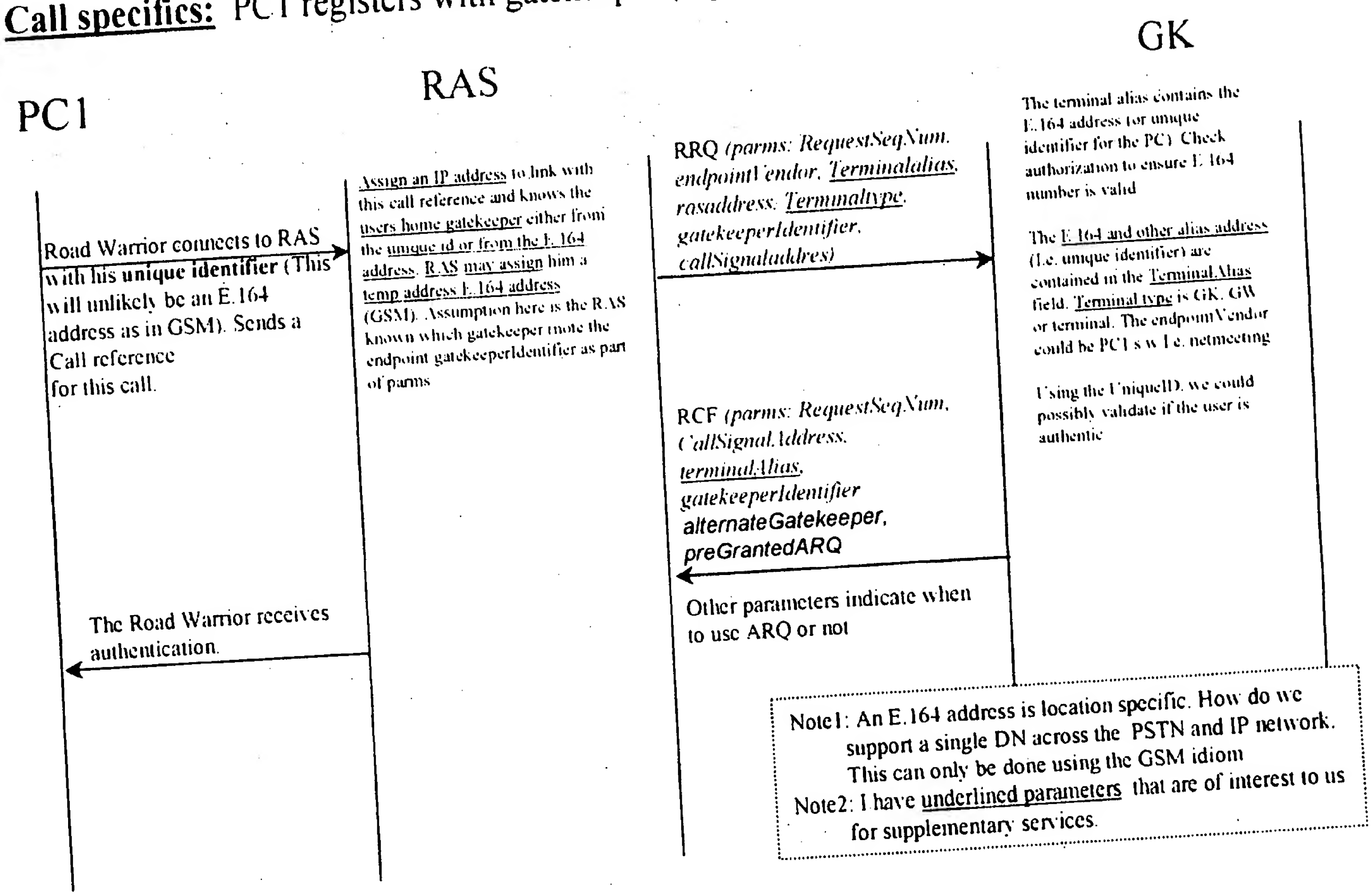
protocolIdentifier *H.225 version*
h245Address *transport address on which the calling endpoint or gatekeeper handles establish of H.245 signaling. Sender is capable of handling H.245 procedures before receiving a CONNECT on the Call Signaling channel.*
sourceAddress *alias addresses for source I.E E.164 number Q.931 Calling Party Number IE.*
sourceInfo *Contains an EndpointType GW GK etc*
destinationAddress *E.164 address, same as Q.931 Called Party Number IE if available. include in the Setup message by version 2 terminals*
destCallSignalAddress *- inform the gatekeeper of the destination terminal's call signaling transport address, redundant in the direct terminal-to-terminal case. If available must be filled in.*
destExtraCallInfo *additional channel calls, i.e. for a 2*64 Kbps on the WAN side. Contain E.164 addresses*
destExtraCRV *- CRVs for the additional SCN calls specified by destExtraCallInfo. Their use is for further study.*
activeMC *- Calling endpoint is under the influence of an active MC*
conferenceID *- unique conference identifier*
conferenceGoal
callIndependentSupplementaryService *- transport of supplementary services APDUs in a non-call related manner*
callServices *- provides information on support of optional Q-series protocols to gatekeeper and called terminal.*
callType *- default value is pointToPoint for all calls*
sourceCallSignalAddress *transport address for the source. Used in the ARQ message by the receiver of the Setup*
remoteExtensionAddress *alias address of a called endpoint. When needed to traverse multiple Gateways.*
callIdentifier *- a globally unique call identifier set by the originating endpoint which can be used to associate RAS signaling with the modified Q.931 signaling used in H.225.0*
h245SecurityCapability *- a set of capabilities the sender can use to secure the H.245 channel*
tokens *This is some data which may be required to allow the operation. The data shall be inserted into the message if available.*
cryptoTokens *- encrypted tokens*
fastStart *- Used only in the fast connect procedure, fastStart supports the signaling needed to open a logical channel. I.E OpenLogicalChannel structure defined in H.245. Sender indicates preferred mode Rx Tx, transport addresses where it expects to receive media streams.*
mediaWaitForConnect *If TRUE, indicates that the recipient of the Setup message shall not transmit media until sending the Connect message.*
canOverlapSend *- If TRUE, sender of Setup shall support overlap sending (set to false)*

Note: In the **ARQ** message **srcInfo**, **destinationInfo** are equivalent to the **SETUP UUIE sourceAddress**, **destinationAddress** respectively.

Detailed Call Flow

Registration Accepted

Call specifics: PC1 registers with gatekeeper (registration accepted)



Registration Rejected

Call specifics: PC1 registers with gatekeeper (registration rejected by gatekeeper)

PC1 | RAS | GK

PC1: Road Warrior connects to RAS with his **unique identifier** (This will unlikely be an E.164 address as in GSM). Sends a Call reference for this call.

What is the user method to uniquely identify themselves?

RAS: Assign an IP address to link with this call reference and knows the users home gatekeeper either from the unique id or from the E.164 address. RAS may assign him a temp address E.164 address (GSM). Assumption here is the RAS known which gatekeeper (note the endpoint gatekeeperIdentifier as part of parms

RRQ *(parms: RequestSeqNum, endpointVendor, Terminalalias, rasaddress, Terminaltype, gatekeeperIdentifier, callSignaladdres,* *willSupplyUUIEs set to false)*

GK: The terminal alias contains the E.164 address (or unique identifier for the PC1. Check authorization to ensure E.164 number is valid.

The E.164 and other alias address (i.e unique identifier) are contained in the TerminalAlias field. Terminal type is GK, GW or terminal. The endpointVendor could be PC1's w i.e netmeeting and version

Authorization rejected the uniqueID not recognized?

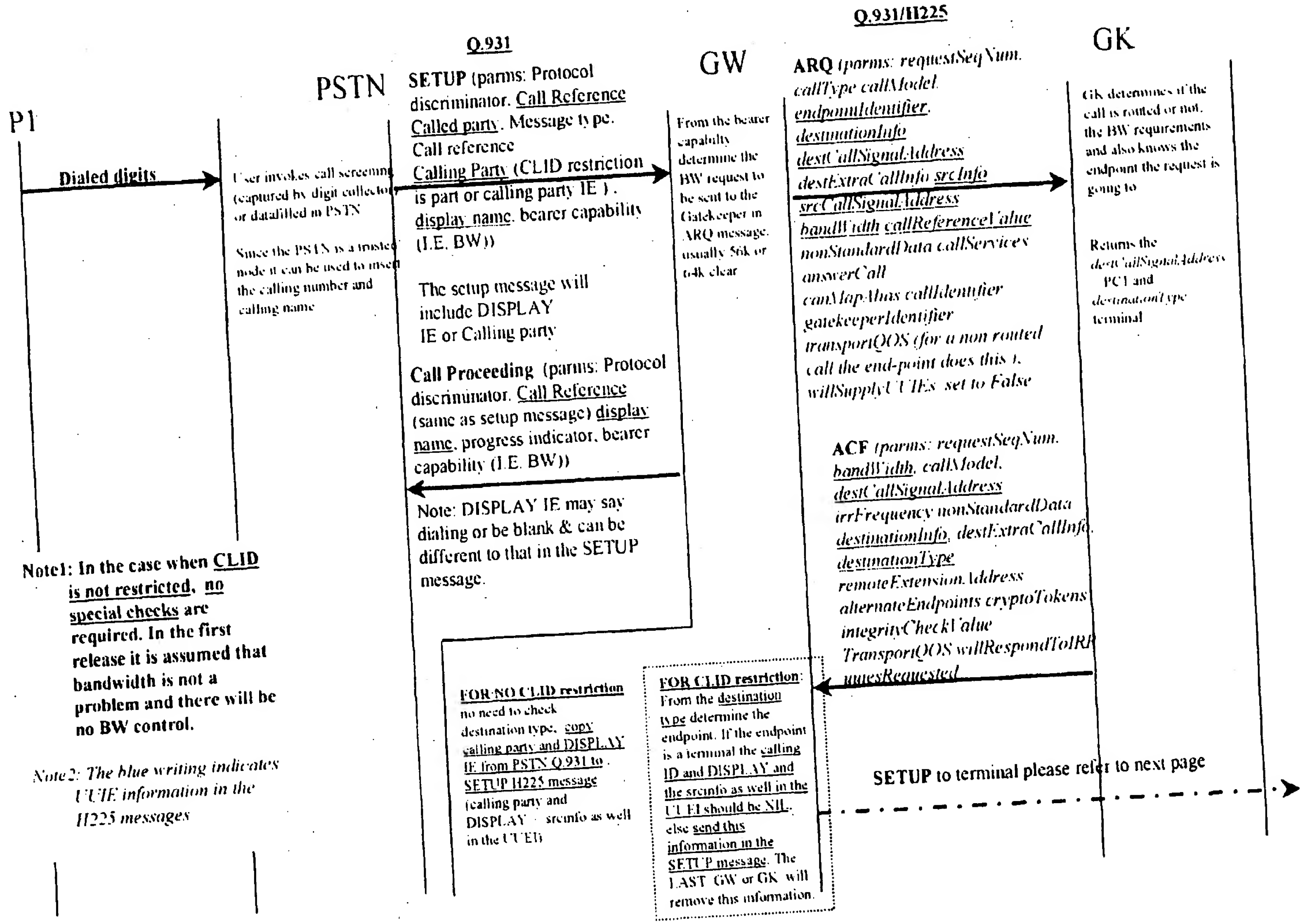
Also when the user registers, can he program the the GK to forward their office phone to his road warrior automatically?

RRJ *(parms: RequestSeqNum, rejectReason, gatekeeperIdentifier)*

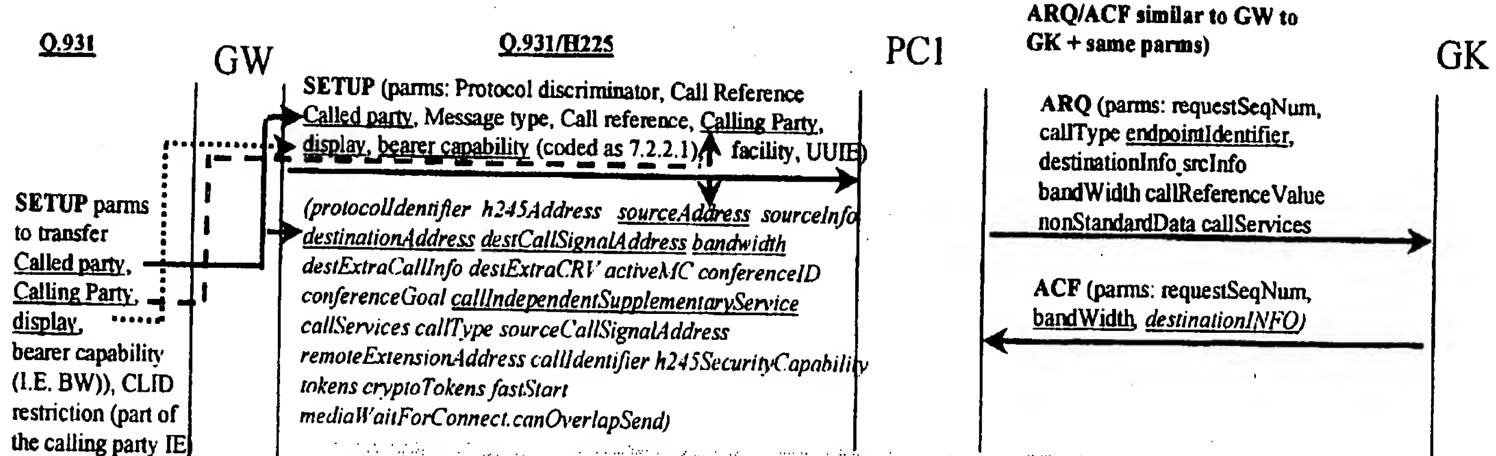
The Road Warrior receives authorization

Note: An E.164 address is location specific.
How do we support a single DN across the PSTN and IP network. This can only be done using the GSM idiom of assigning a temporary E.164(done by RAS). User device has 3 ids, its own uniqueid, one assigned by RAS and an IP assigned by RAS. All must be sent to the GK.

P1 calls PC1 - Page 1



P1 calls PC1 - Page 2

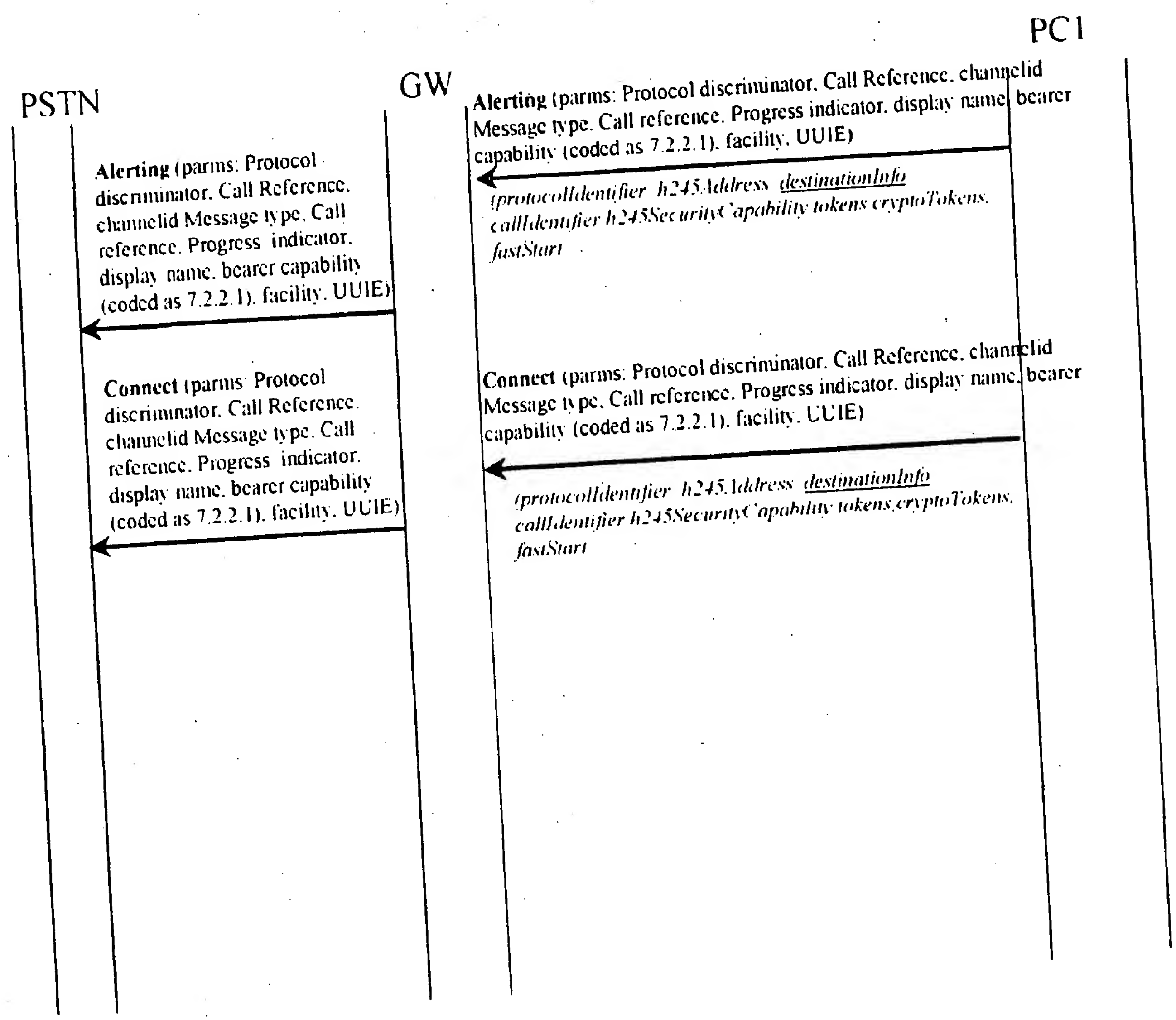


Note1: This call reference is local between the GW and PC1.
Note2: The Italic parms indicate parms contained within the UUIE.
Note3: DISPLAY is the same as CALLING NAME in supplementary services

Note4: **Problem:** CLID restriction, Octet3a in Q.931 H.225 Setup is not allowed.
This is part of the Calling Party IE. The dotted green line indicates the fields the Calling Party, DISPLAY IE can be transferred Calling Party/

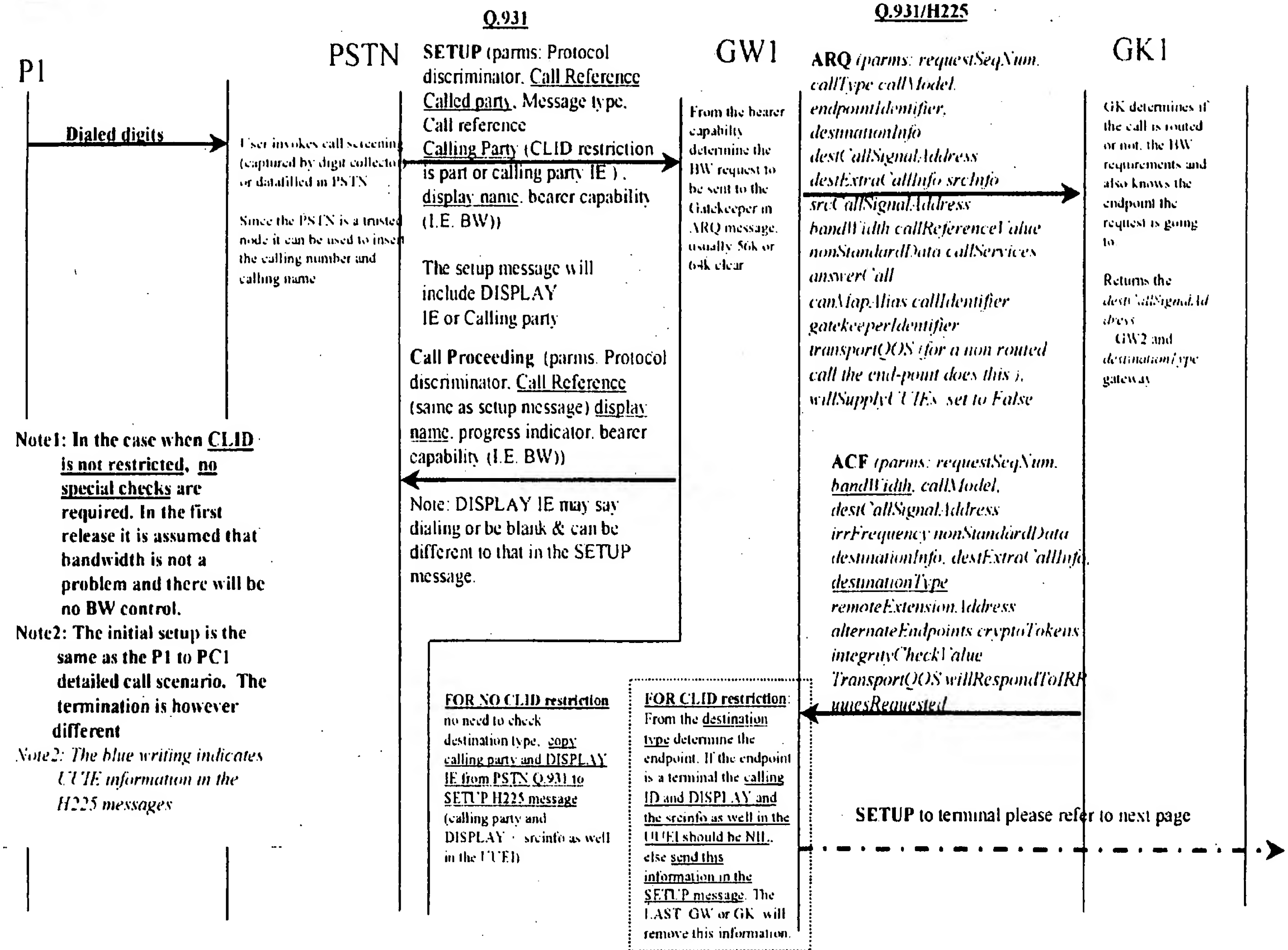
- If terminating endpoint is a terminal or MCU + CLID RESTRICTION in the calling party then GW leaves these fields blank
- If the no CLID restriction, OK to transfer fields
- If the case the endpoint is a intermediate node such as a GW or a GK & CLID restriction is requested then we have 4 options:
  - A) Transfer the fields and add a *callIndependentSupplementaryService APDU (Call Restriction APDU)* for call restriction (as defined in H450.1 ROS objects). This is the best way as we comply with H450 and H225 standards but requires work in the GW/GK (this implies Nortel) and the last node in the call will remove the calling number and display. May also require work in the standards body.
  - B) Leave the fields blank as these are optional Q.931 fields anyway. This is the simplest method requiring no work. However, all this work is mote if the PC terminal vendors add user information into the UserIndication field.
  - C) Copy the CLID restriction as part of the Calling party IE, have standard modified to H.225+ (this would means standards work and is propriety to NT). May also require work in the standards body.
  - D) Use the User Indication field in the UUIE. Again this will require work in the GW.

P1 calls PC1 - Page 3

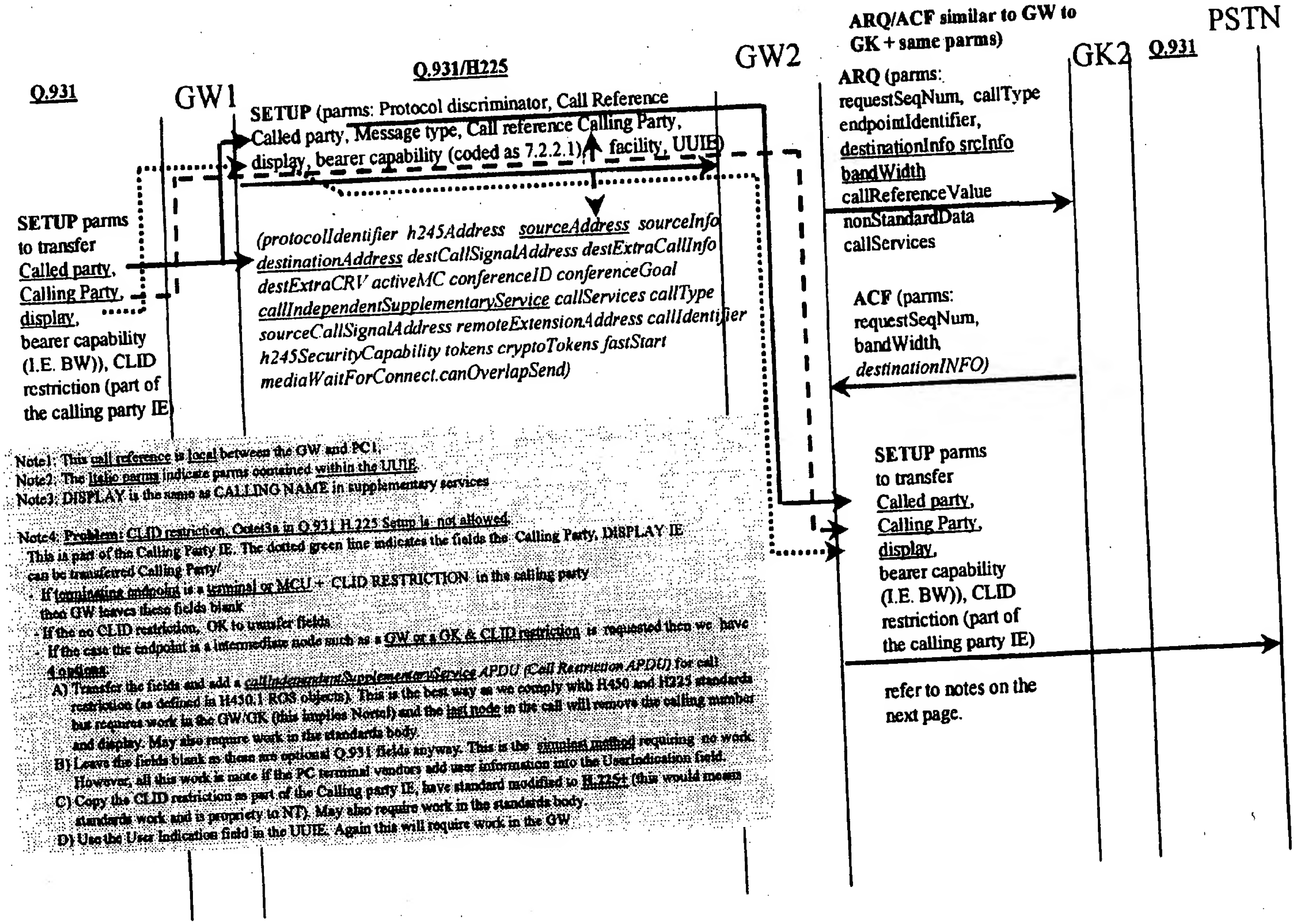


P1 PSTN1 calls P5 PSTN 2 - Page 1

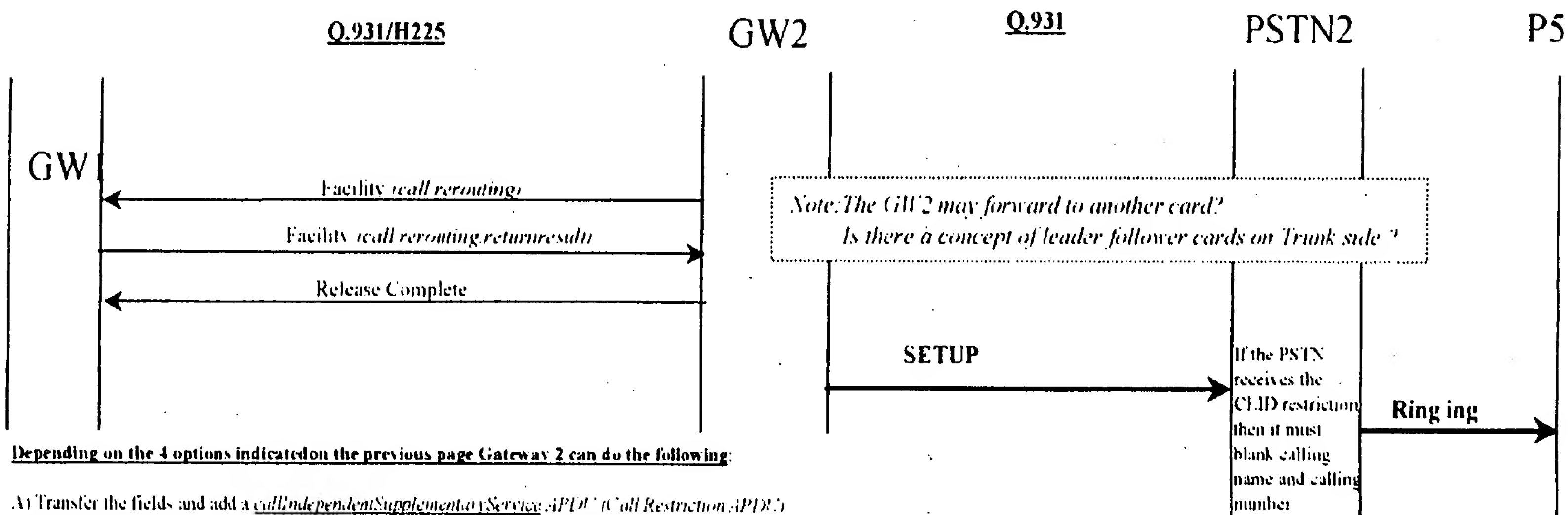
Call specifics: Also known as LONG DISTANCE BY-PASS.



P1 PSTN1 calls P5 PSTN 2 - Page 2



P1 PSTN1 calls P5 PSTN 2 - Page 3



Depending on the 4 options indicatedon the previous page Gateway 2 can do the following:

A) Transfer the fields and add a *callIndependentSupplementaryService APDU (Call Restriction APDU)*
- GW 2 has the corresponding APDU implemented and readds the CLID restriction field to the Q931 setup message (calling party IE). This is the most difficult of all the options but the most standards based.

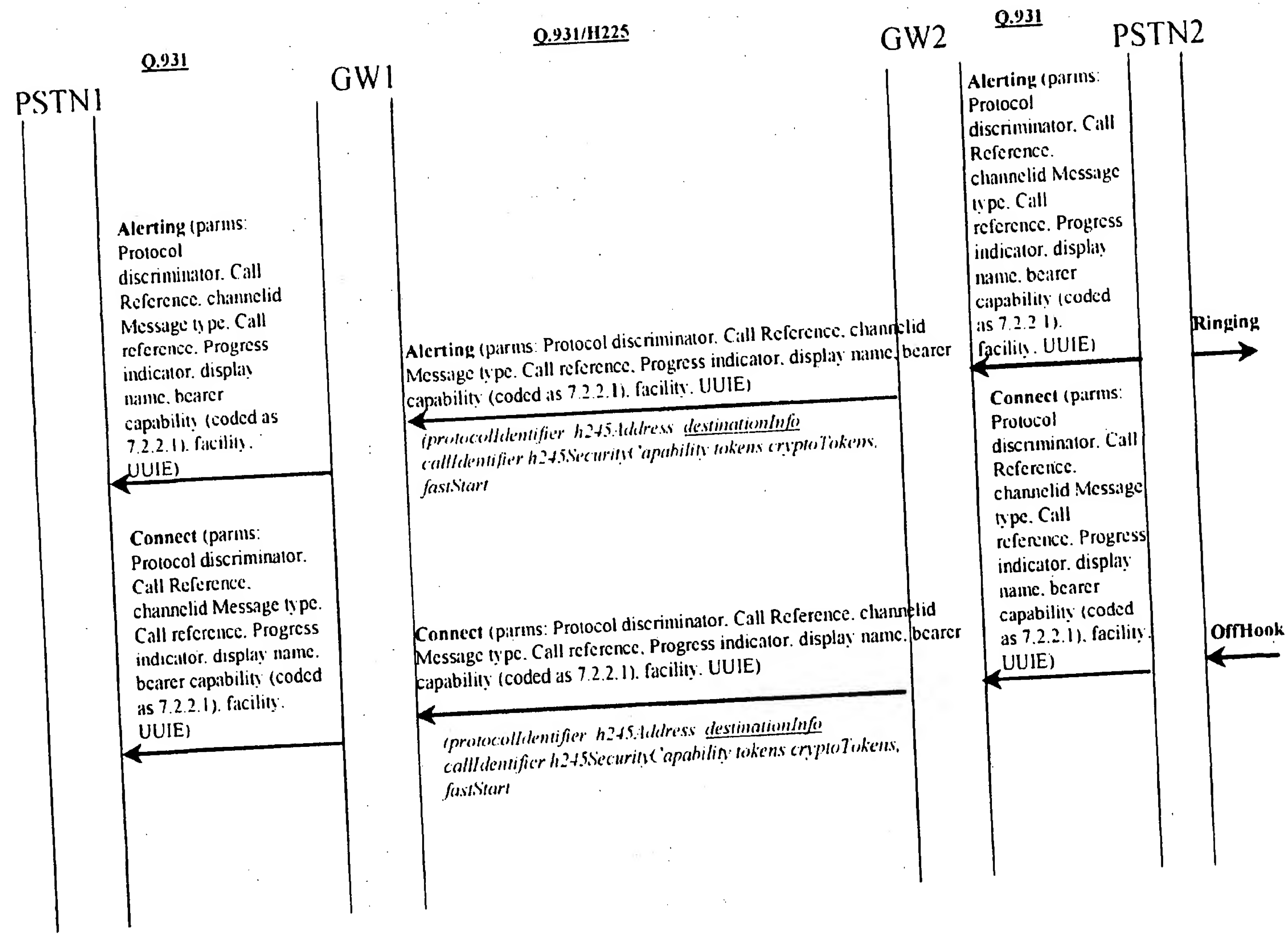
B) Leave the fields blank as these are optional Q.931 fields anyway. This is the simplest method requiring no work.
- No work on GW2. CLID restriction no required to be added

C) Copy the CLID restriction as part of the Calling party IE, have standard modified to **H.225+**
- Minimum work to copy fields fields across from H225 to Q931

D) Use the User Indication field in the UUIE. Again this will require work in the GW.
- Work required at the GW. Still no standards based and could be a limitation on the number of characters that can be placed in the UserIndication field.

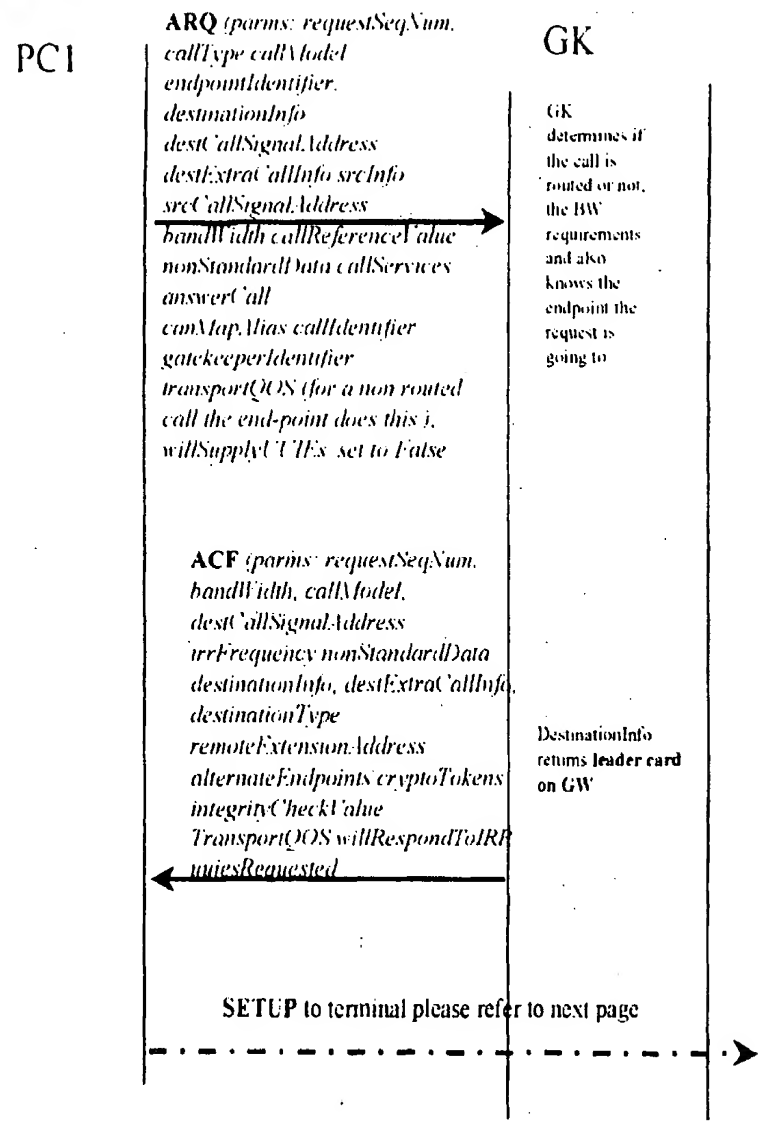
I would Recommend Option B for simplicity

P1 PSTN1 calls P5 PSTN 2 - Page 4

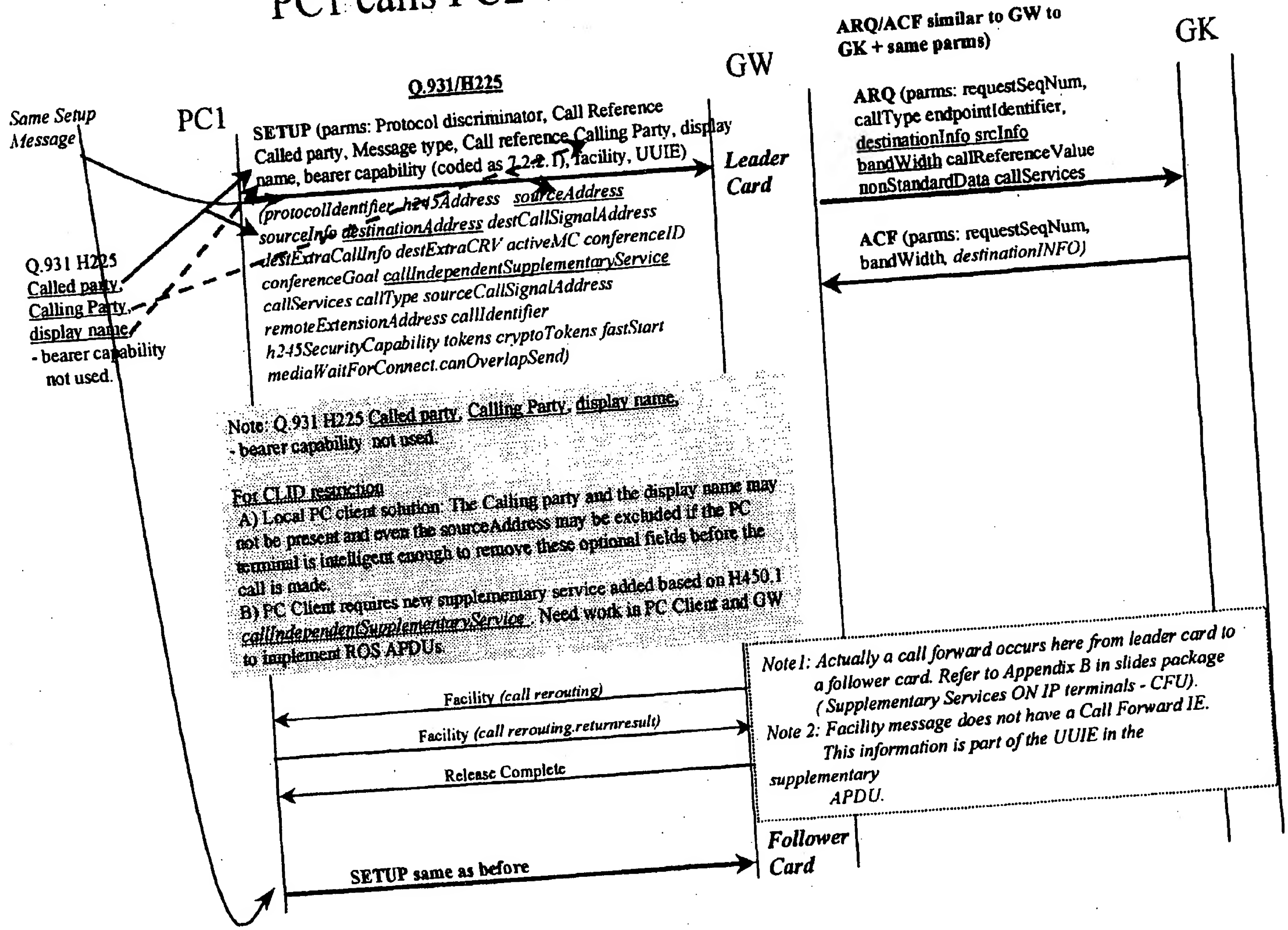


PC1 calls PC2 (IP terminal to IP terminal) via GW- Page 1

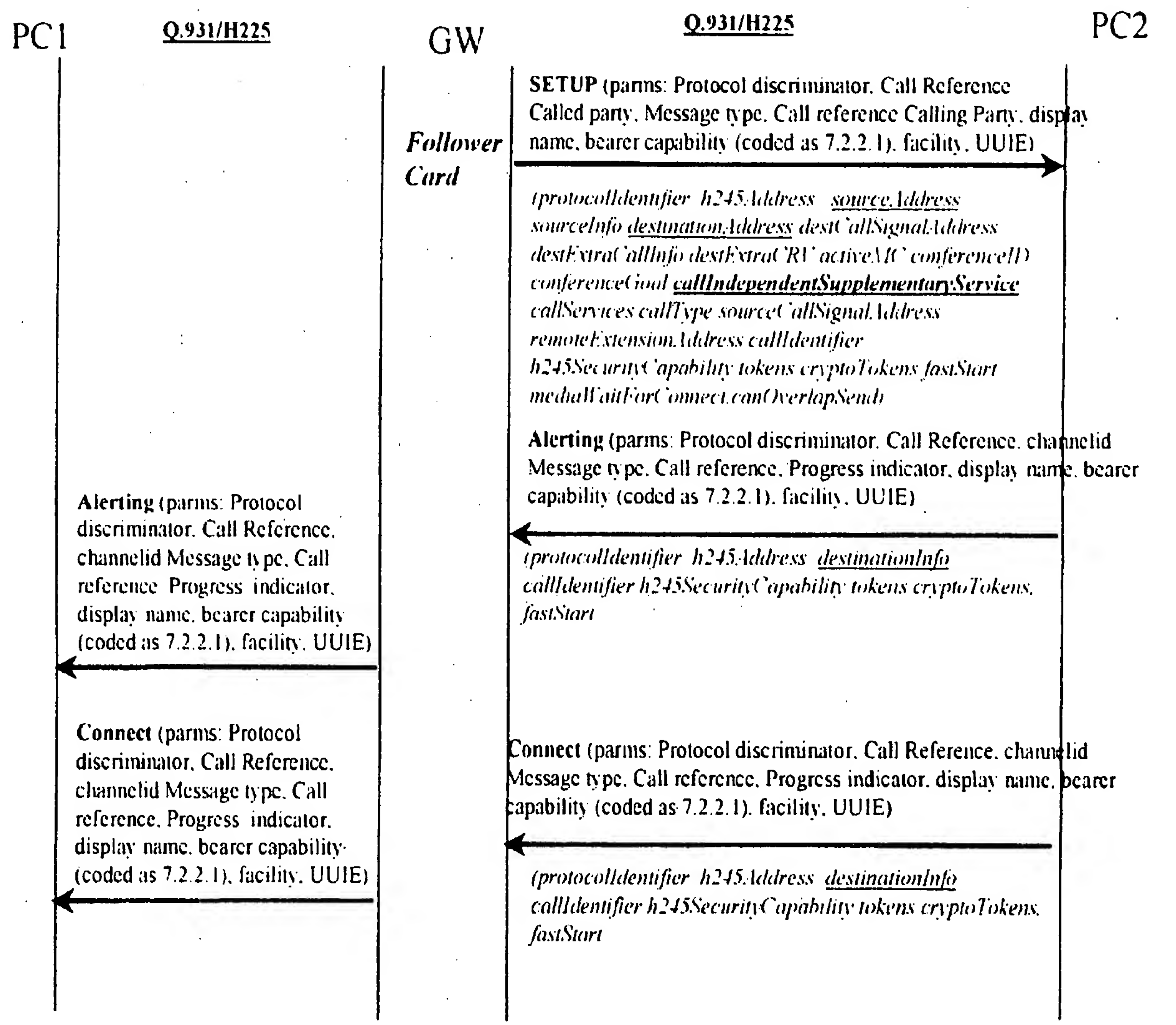
Call specifics: The GW is used to make use of Billing records software available in the MMCS.



PC1 calls PC2 via GW - Page 2

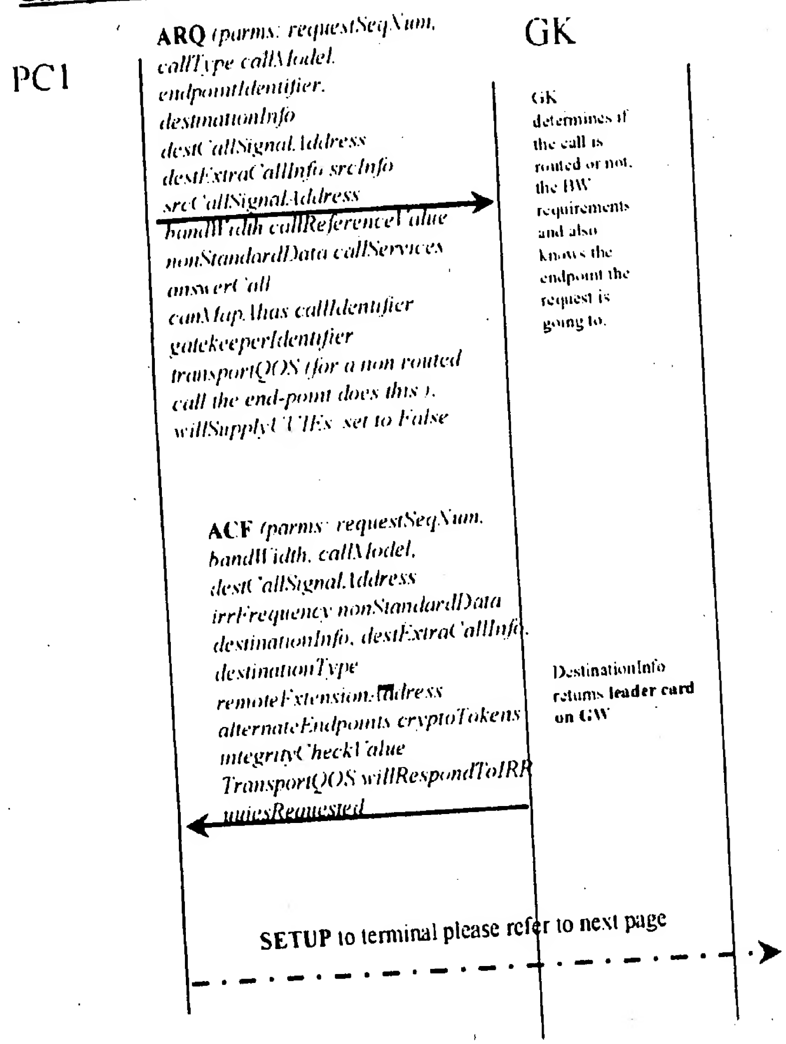


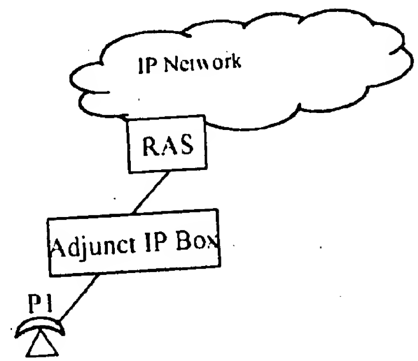
PC1 calls PC2 via GW - Page 3



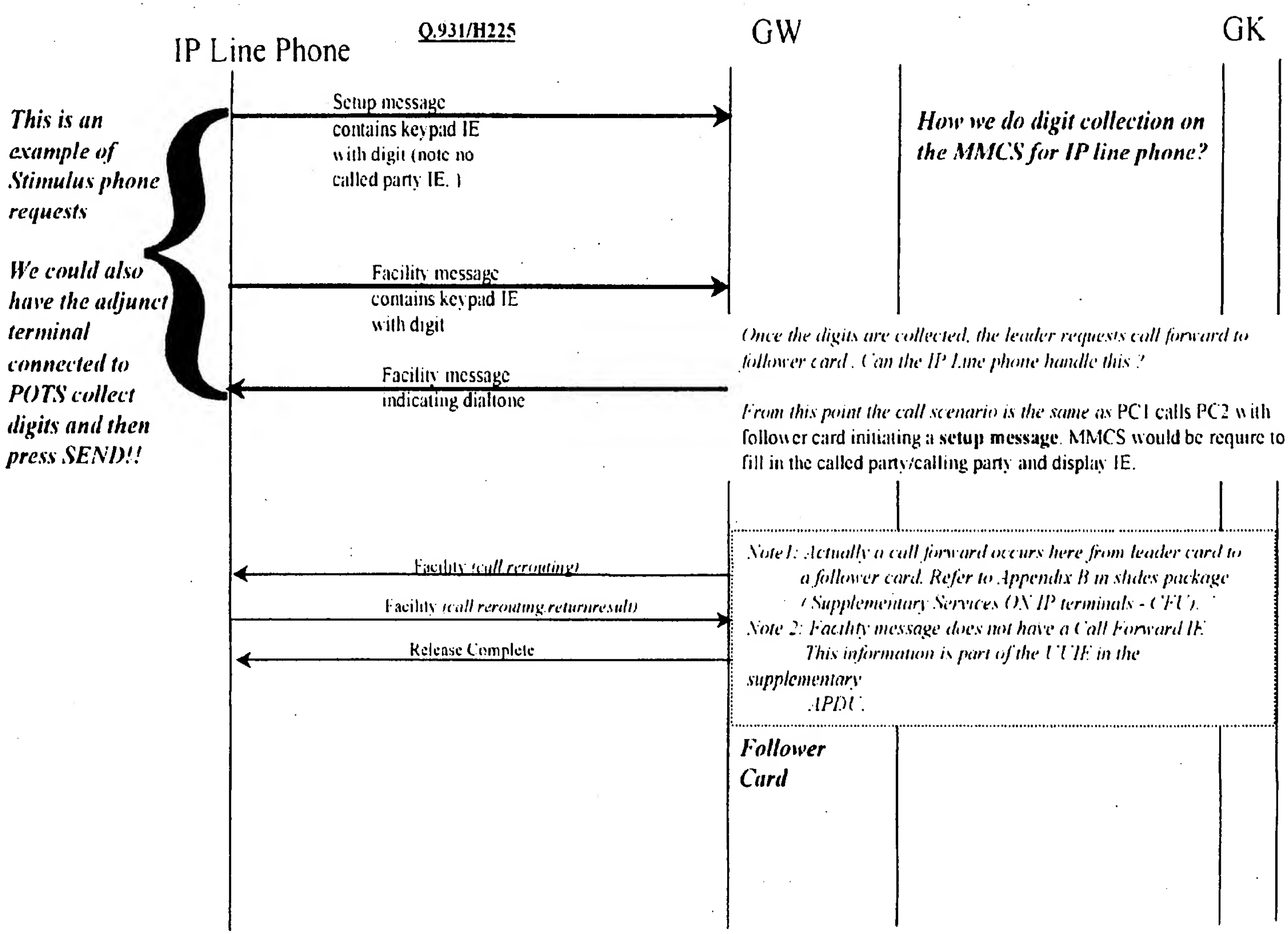
IP LINE Phone calls PC2 (IP terminal to IP terminal) via GW- Page 1

Call specifics: This is a POTS phone that is connected to an IP adjunct on the IP extranet

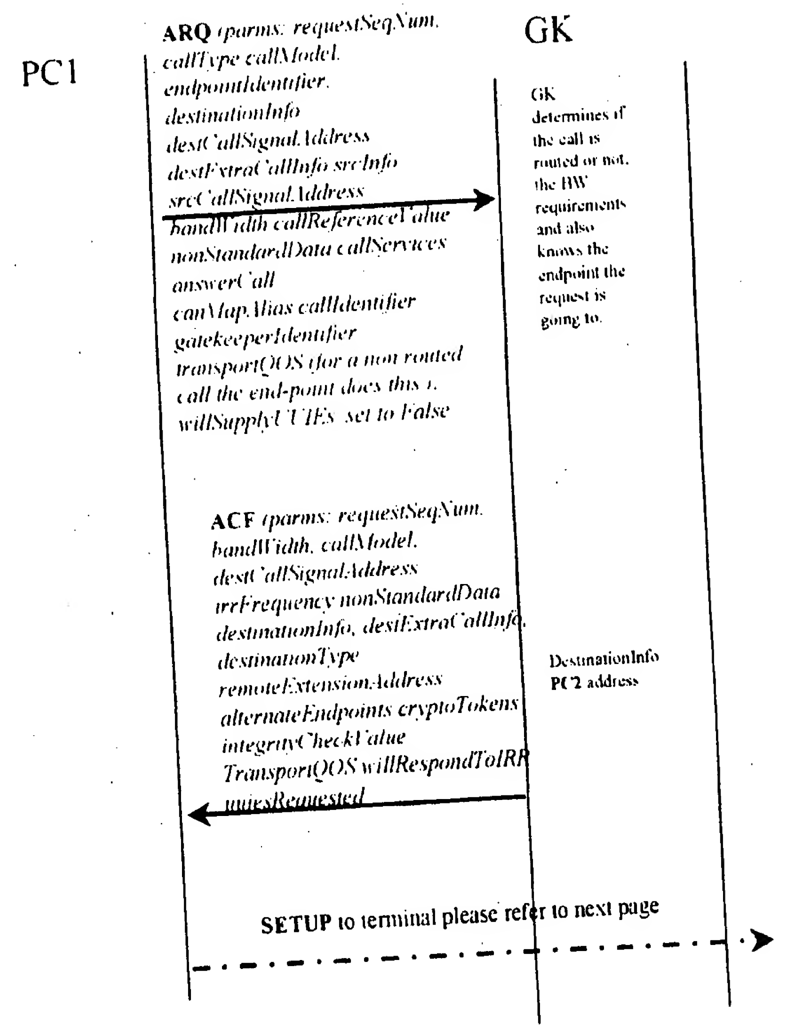




IP Line Phone calls PC2 via GW - Page 2

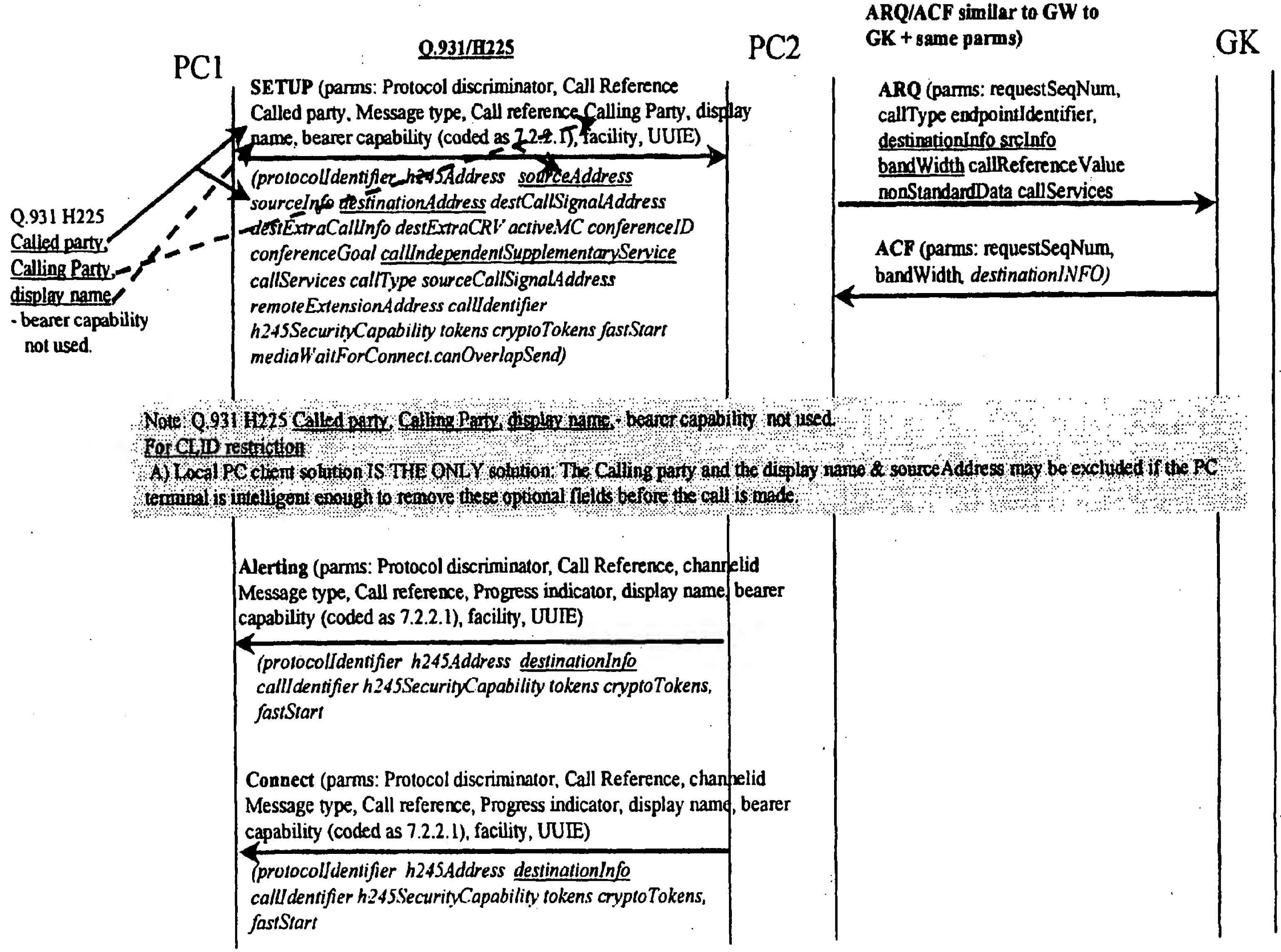


PC1 calls PC2 DIRECT - Page 1



Note: How do we handle Billing if not through the Gateway?

PC1 calls PC2 Direct



Claims

1. A gateway for use between between an IP network and another network, the gateway being adapted to handle calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the gateway being further adapted to provide at least one supplementary service for calls to or from an IP terminal device.

2. The gateway according to claim 1, wherein the supplementary service is chosen from at least one of:
originating restrictions;
   - a terminating restriction;
   - call forwarding;
   - calling line identification;
   - CLID restriction;
   - calling name display;
   - call transfer.

3. The gateway according to any previous claim, wherein the gateway is adapted to provide the supplementary service on a call between two IP terminal devices and/or to provide the supplementary service on a call between an IP terminal device and a terminal device connected to the other network.

4. The gateway according to any previous claim, wherein the gateway comprises a shared pool of ports on the line side which are usable for a connection to an IP terminal device.

5. The gateway according to any previous claim, wherein the gateway is adapted to dynamically associate an IP terminal device client's subscriber data with a call.

6. The gateway according to any previous claim, wherein the gateway is adapted to perform address resolution for calls to IP terminal devices.

7. The gateway according to any previous claim, wherein the gateway is integrated with a switch.

8. An IP network for connection to another network, the IP network being adapted for handling calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the network being further adapted to provide at least one supplementary service for calls to or from an IP terminal device.

9. The IP network according to claim 8, wherein the supplementary service is chosen from at least one of:
originating restrictions;
   - a terminating restriction;
   - call forwarding;
   - calling line identification;
   - CLID restriction;
   - calling name display;
   - call transfer.

10. The IP network according to claim 8 or 9, wherein the network is adapted to provide the supplementary service on a call between two IP terminal devices and/or is adapted to provide the supplementary service on a call between an IP terminal device and a terminal device connected to the other network.

11. The IP network according to any of claims 8 to 10, wherein the network is adapted to dynamically associate an IP terminal device client's subscriber data with a call.

12. The IP network according to any of claims 8 to 11, wherein a voice call between two IP terminal devices without double encoding/decoding of the voice data.

13. The IP network according to any of claims 8 to 12, further comprising a gateway, the gateway being adapted to

provide the supplementary service.

14. The IP network according to any of claims 8 to 13, wherein the gateway comprises a shared pool of ports on the line side which are usable for a connection to an IP terminal device.

15. The IP network according to any of claims 8 to 14, wherein the network is adapted to route call control signals for a call between two IP terminal devices through the gateway or the IP network is adapted to route call control signals for a call between two IP terminal devices through the IP network and call signaling though the gateway.

16. A method of operating a gateway between an IP network and another network, the gateway being adapted to handle calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the method including the step of providing at least one supplementary service for calls to or from an IP terminal device.

17. The method according to claim 16, wherein the supplementary service is chosen from at least one of: originating restrictions;

- a terminating restriction;
- call forwarding;
- calling line identification;
- CLID restriction;
- calling name display;
- call transfer.

18. The method according to claim 16 or 17, wherein the supplementary service is provided on a call between two IP terminal devices and/or is provided on a call between an IP terminal device and a terminal device connected to the other network.

19. The method according to any of the claims 16 to 18, further comprising the step of dynamically associating an IP terminal device client's subscriber data with a call.

20. A method of operating an IP network connected to another network, the IP network handling calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the method comprising the step of providing at least one supplementary service for calls to or from an IP terminal device.

21. The method according to claim 20, wherein the supplementary service is chosen from at least one of: originating restrictions:

- a terminating restriction;
- call forwarding;
- calling line identification;
- CLID restriction;
- calling name display;
- call transfer.

22. The method according to claim 20 or 21, further comprising the step of dynamically associating an IP terminal device client's subscriber data with a call.

23. The method according to any of claims 20 to 22, further comprising the step of routing a voice call between two IP terminal devices without double encoding/decoding of the voice data.

24. A gateway between an IP network and another network, the gateway handling calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the gateway comprising a shared pool of ports on the line side which are usable for a connection to an IP terminal device.

25. The gateway according to claim 24, wherein the gateway is adpated to dynamically associate an IP terminal device

client's subscriber data with a call.

26. A method of operating IP network having a gateway between the IP network and another network, the gateway handling calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the method including the steps of:
routing call signaling for a call between two IP terminals though the gateway and routing voice traffic between two IP terminals without pasing via the gateway.

27. An IP network having a gateway between an IP network and another network, the gateway handling calls between IP terminal devices connected to the IP network as well as calls between an IP terminal device and a terminal device connected to the other network, the method including the steps of:
routing call signaling for a call between two IP terminals though the gateway and routing voice traffic between two IP terminals without pasing via the gateway.

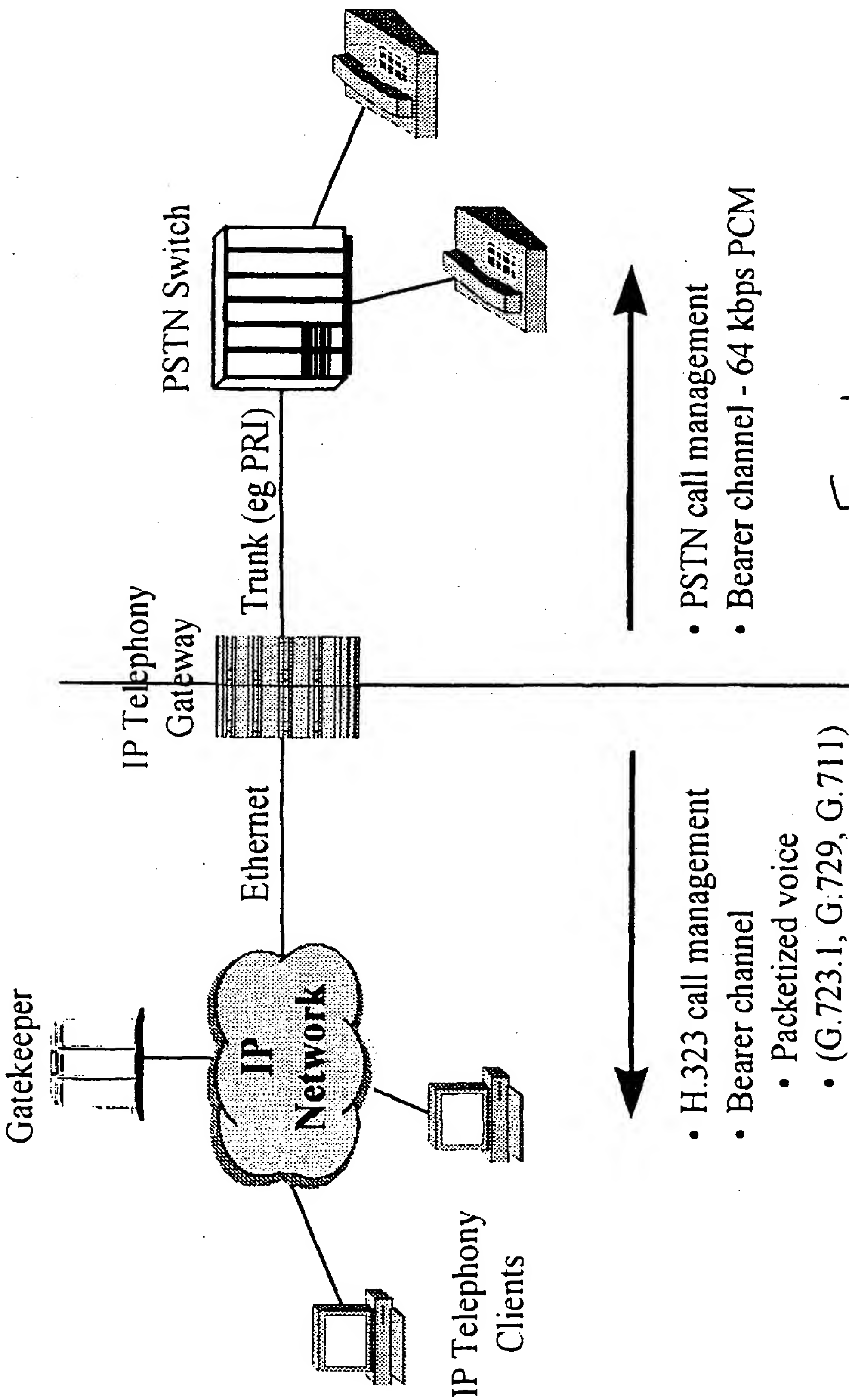
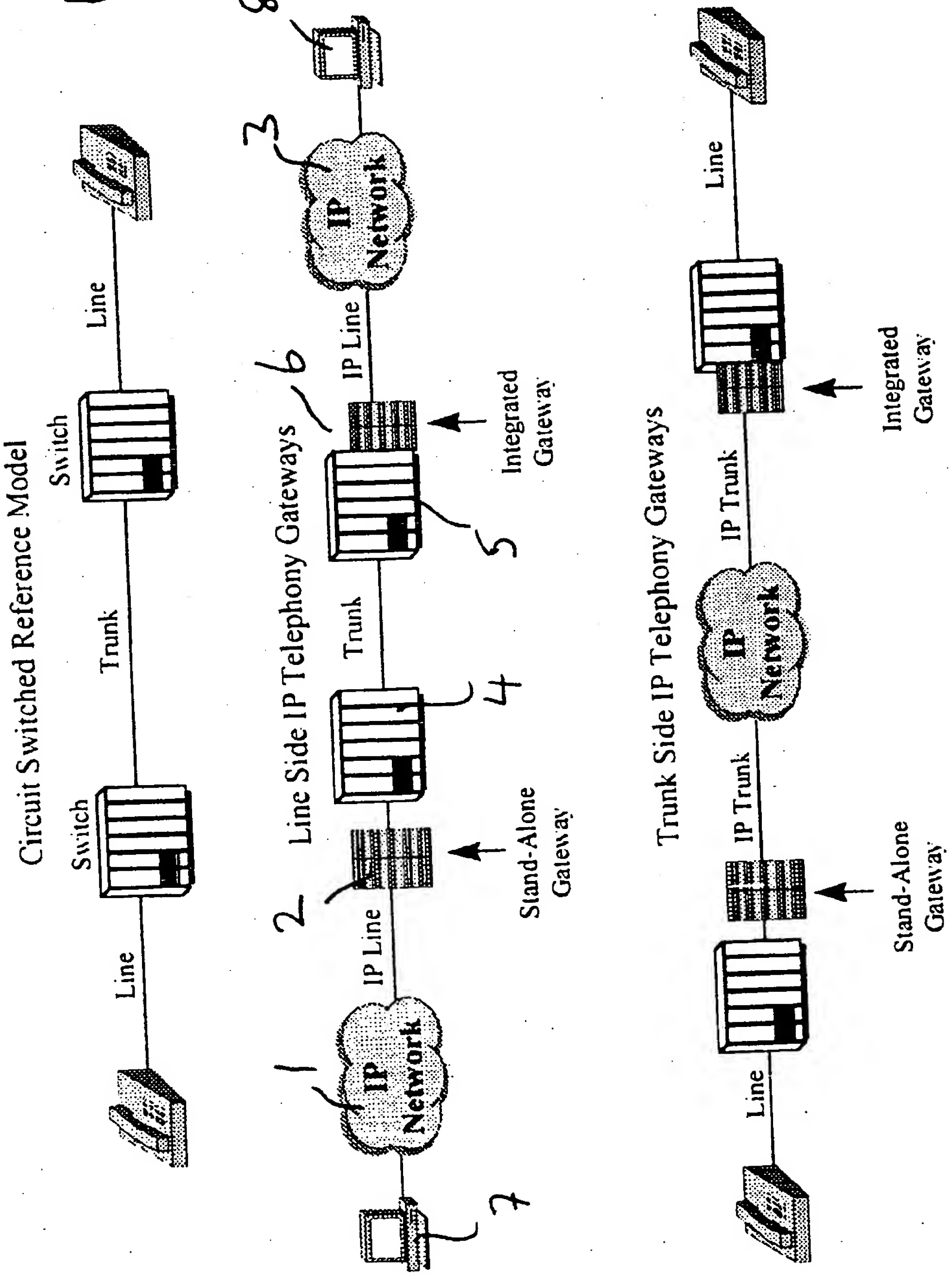

Gatekeeper
IP Network
IP Telephony Clients
Ethernet
IP Telephony Gateway
Trunk (eg PRI)
PSTN Switch
• H.323 call management
• Bearer channel
• Packetized voice
• (G.723.1, G.729, G.711)
• PSTN call management
• Bearer channel - 64 kbps PCM

Fig. 1

Fig. 2A

Fig. 2B

Fig. 2C



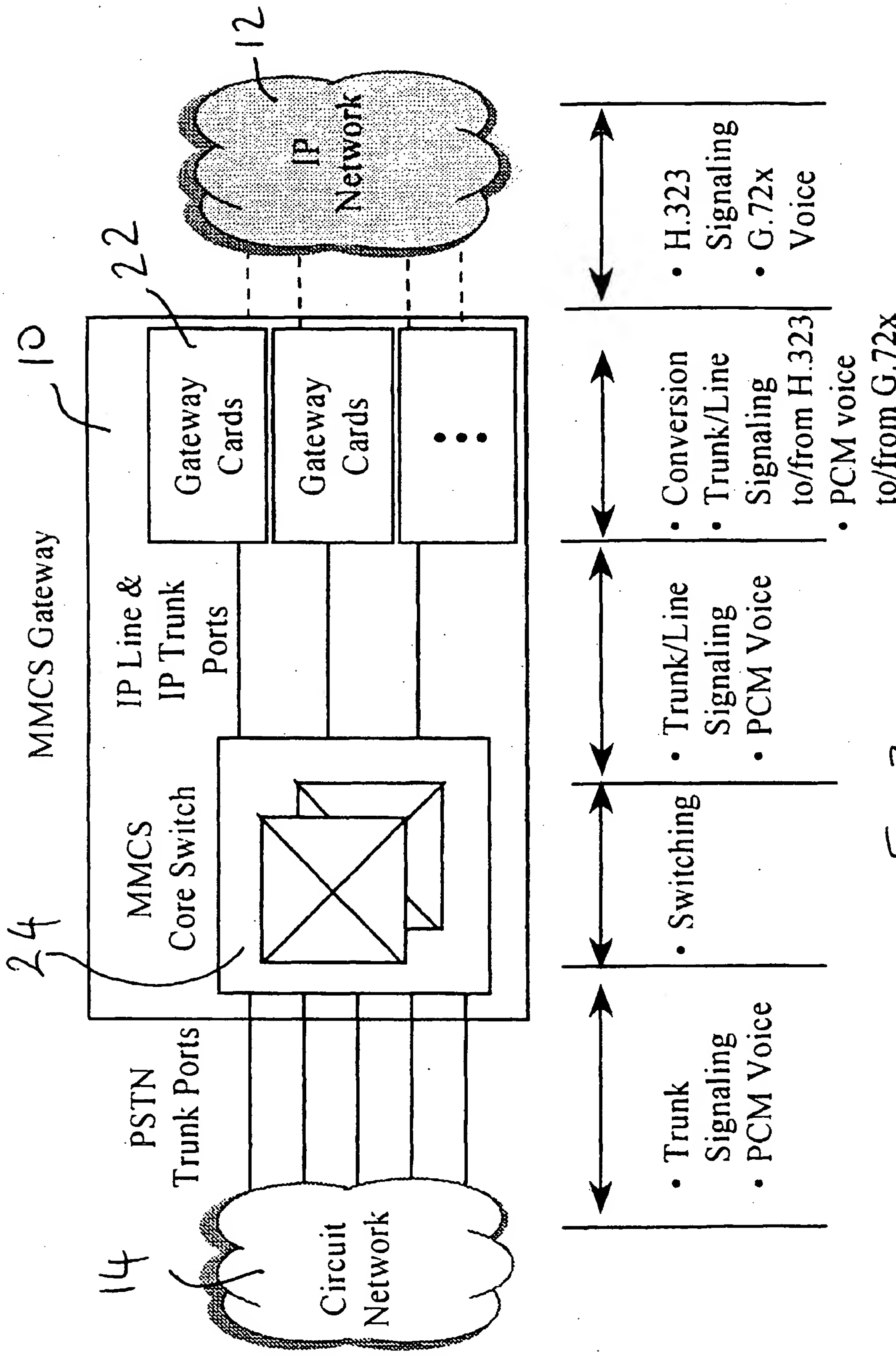

12
IP Network
22
10
Gateway Cards
Gateway Cards
MMCS Gateway
IP Line & IP Trunk Ports
MMCS Core Switch
24
PSTN Trunk Ports
14
Circuit Network
• H.323 Signaling
• G.72x Voice
• Conversion
• Trunk/Line Signaling to/from H.323
• PCM voice to/from G.72x
• Trunk/Line Signaling
• PCM Voice
• Switching
• Trunk Signaling
• PCM Voice

Fig. 3

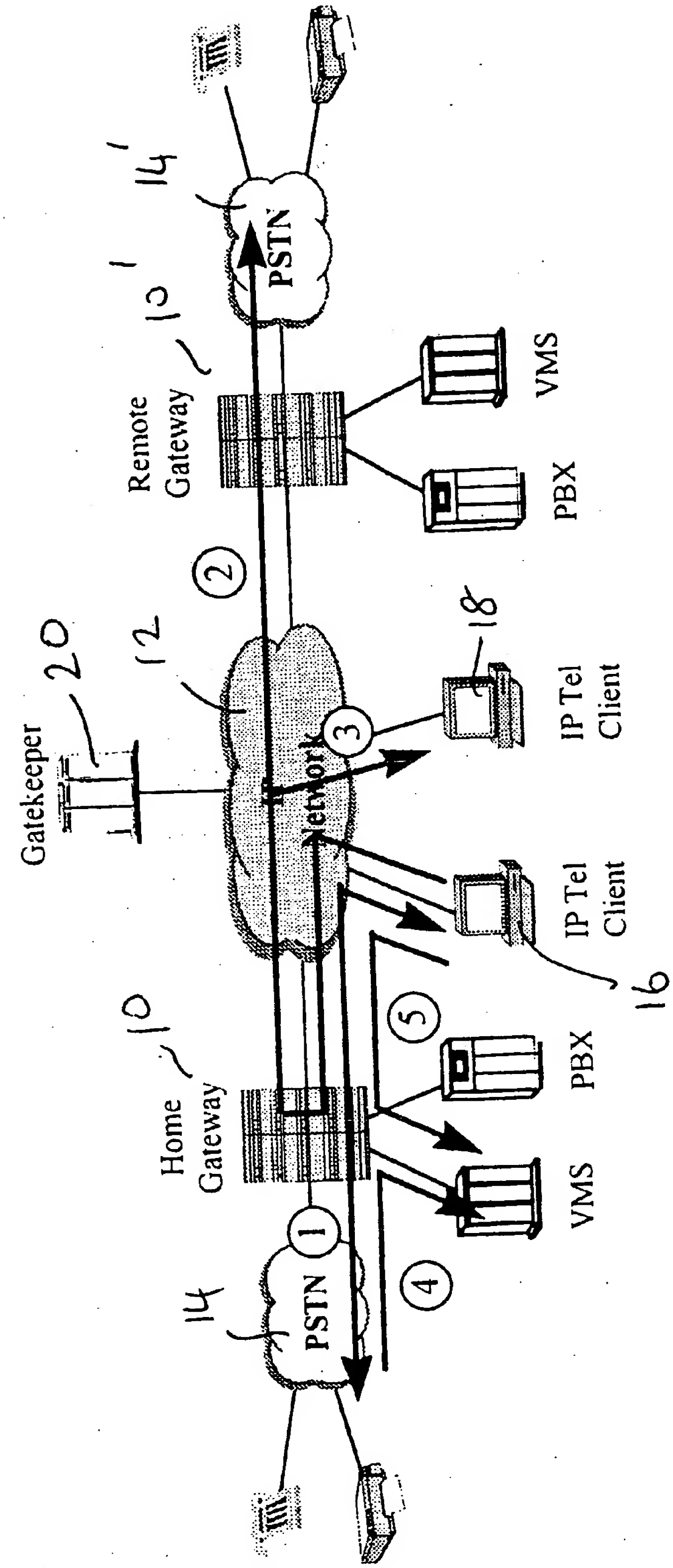

Gatekeeper
20
12
Network
PSTN
14'
10'
Remote
Gateway
VMS
PBX
2
3
18
IP Tel
Client
IP Tel
Client
16
5
PBX
Home
Gateway
10
VMS
1
4
PSTN
14

Fig. 4A

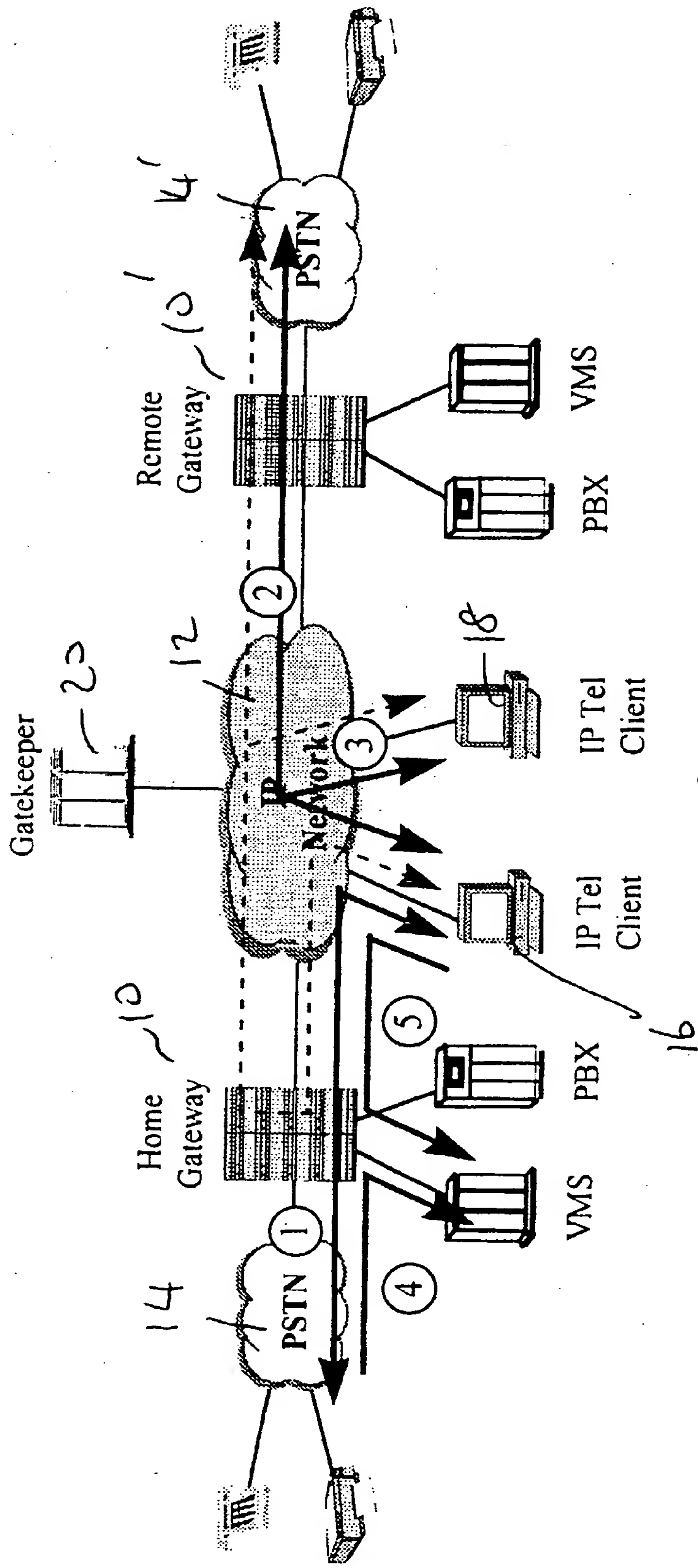
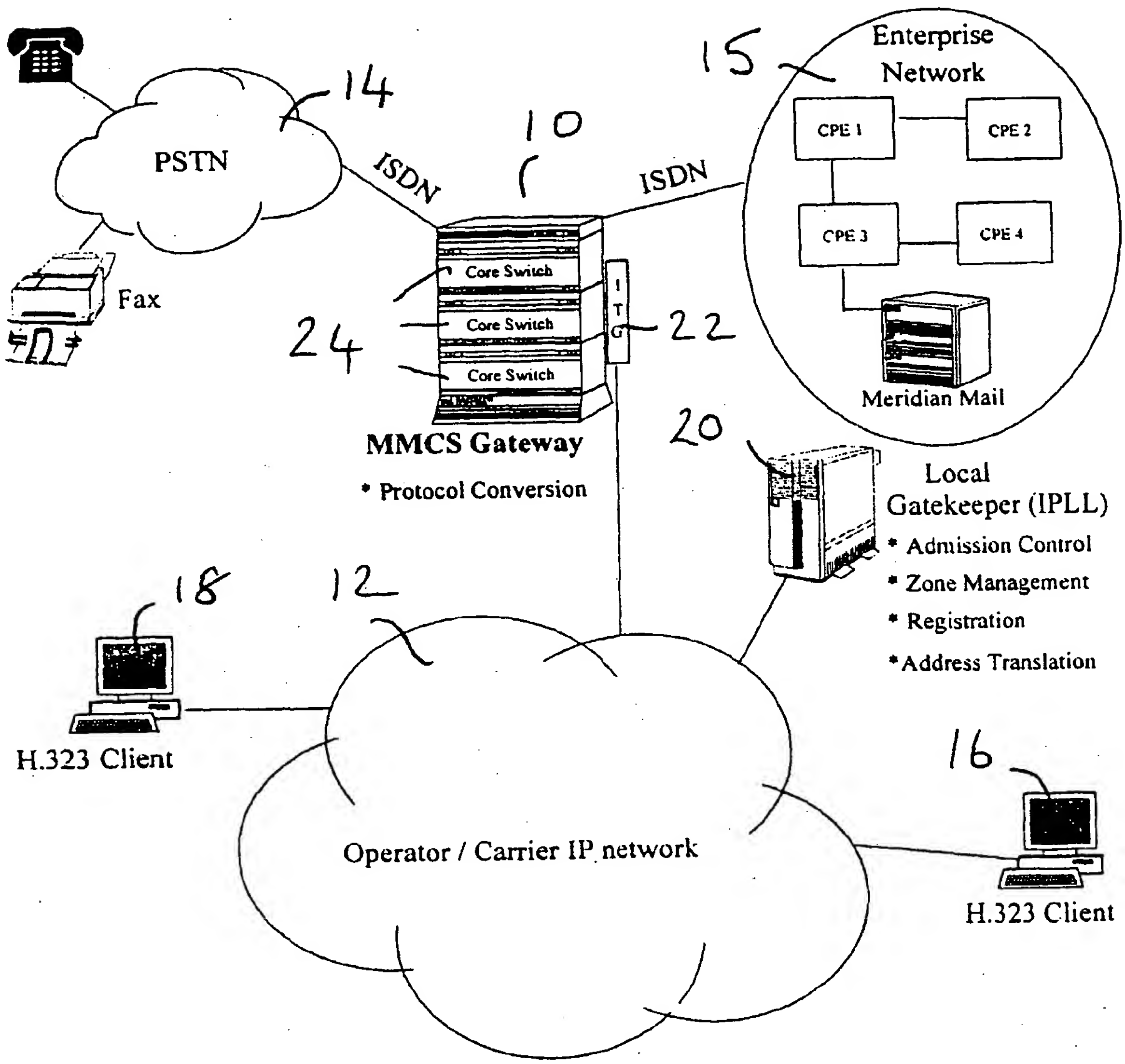

Gatekeeper
23
12
IP Network
2
3
Remote Gateway
10'
4'
PSTN
VMS
PBX
IP Tel Client
18
IP Tel Client
16
Home Gateway
10
5
PBX
VMS
1
4
PSTN
14

Fig. 4B



PSTN
14
Fax
ISDN
10
ISDN
15
Enterprise
Network
CPE 1
CPE 2
CPE 3
CPE 4
Meridian Mail
Core Switch
Core Switch
Core Switch
I
T
G
22
24
MMCS Gateway
* Protocol Conversion
20
Local
Gatekeeper (IPLL)
* Admission Control
* Zone Management
* Registration
*Address Translation
18
12
H.323 Client
Operator / Carrier IP network
16
H.323 Client

Fig. 5

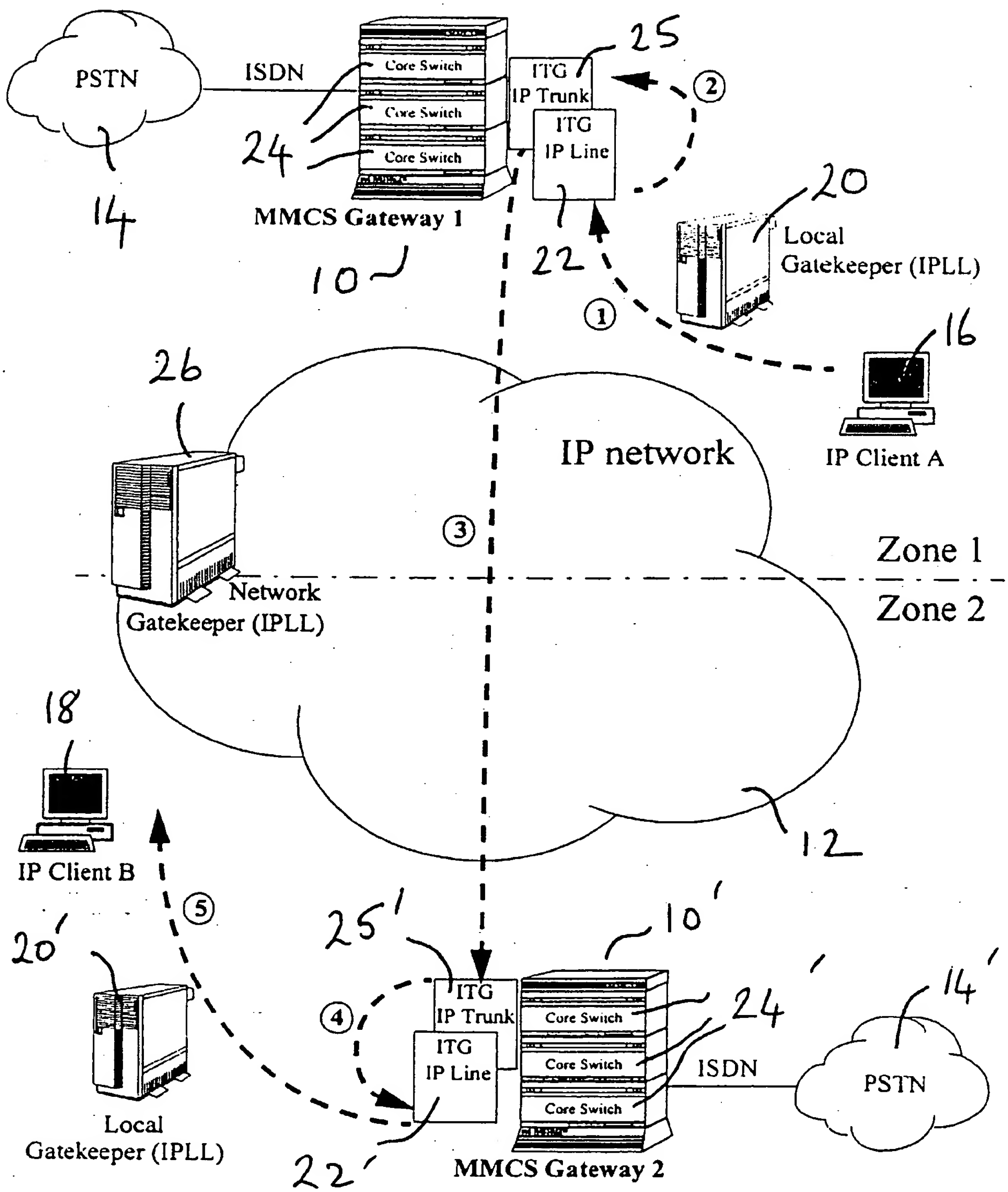

PSTN
ISDN
Core Switch
Core Switch
Core Switch
ITG
IP Trunk
ITG
IP Line
25
2
24
14
MMCS Gateway 1
10
22
20
Local
Gatekeeper (IPLL)
1
16
26
IP network
IP Client A
3
Zone 1
Zone 2
Network
Gatekeeper (IPLL)
18
IP Client B
12
5
25'
10'
20'
ITG
IP Trunk
4
ITG
IP Line
Core Switch
Core Switch
Core Switch
24'
14'
ISDN
PSTN
Local
Gatekeeper (IPLL)
22'
MMCS Gateway 2

Fig. 6

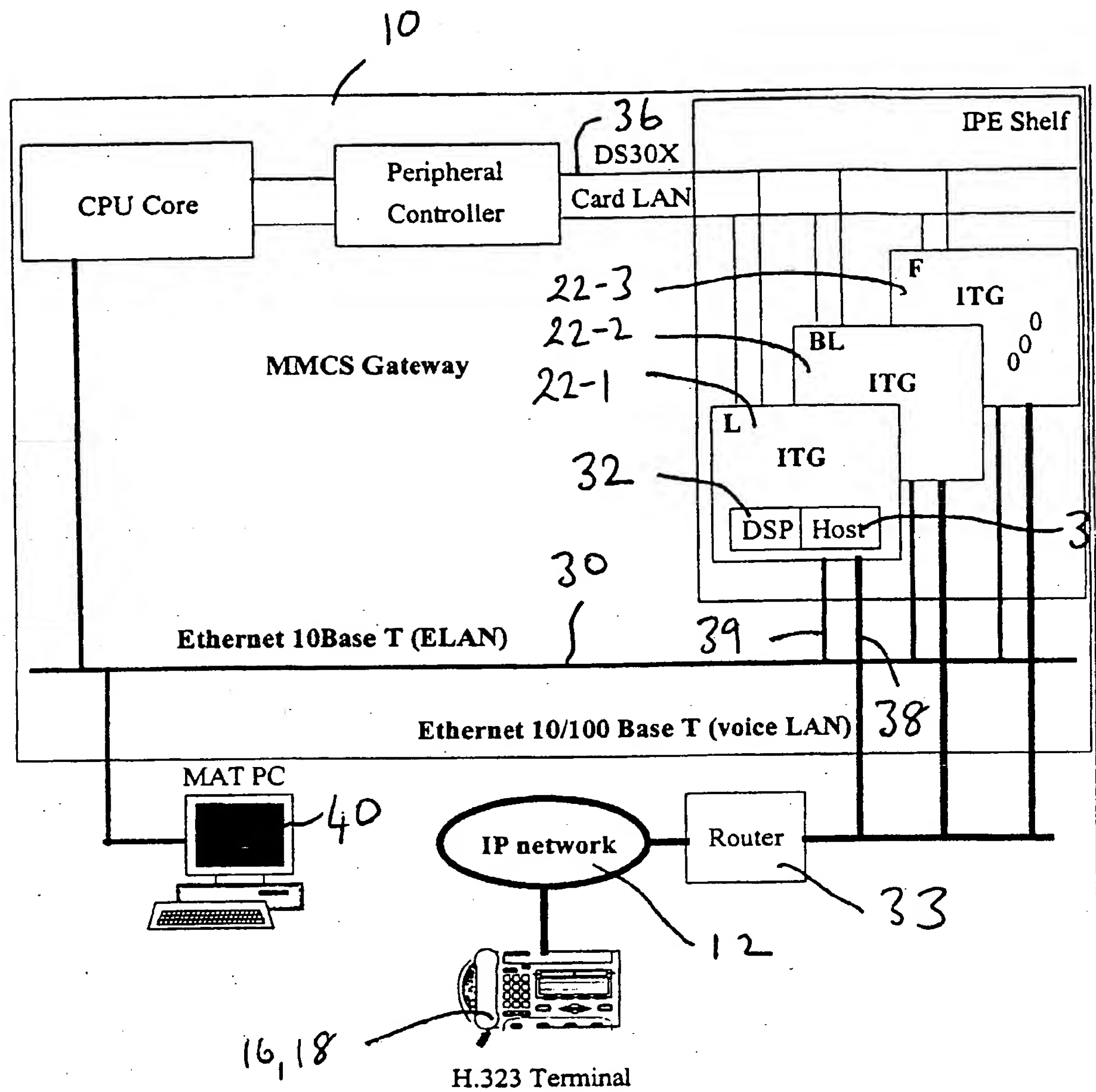

10
36
DS30X
Card LAN
IPE Shelf
CPU Core
Peripheral
Controller
22-3
22-2
22-1
F
ITG
BL
ITG
L
ITG
MMCS Gateway
32
DSP
Host
34
30
39
Ethernet 10Base T (ELAN)
38
Ethernet 10/100 Base T (voice LAN)
MAT PC
40
IP network
Router
33
12
16,18
H.323 Terminal

Fig. 7

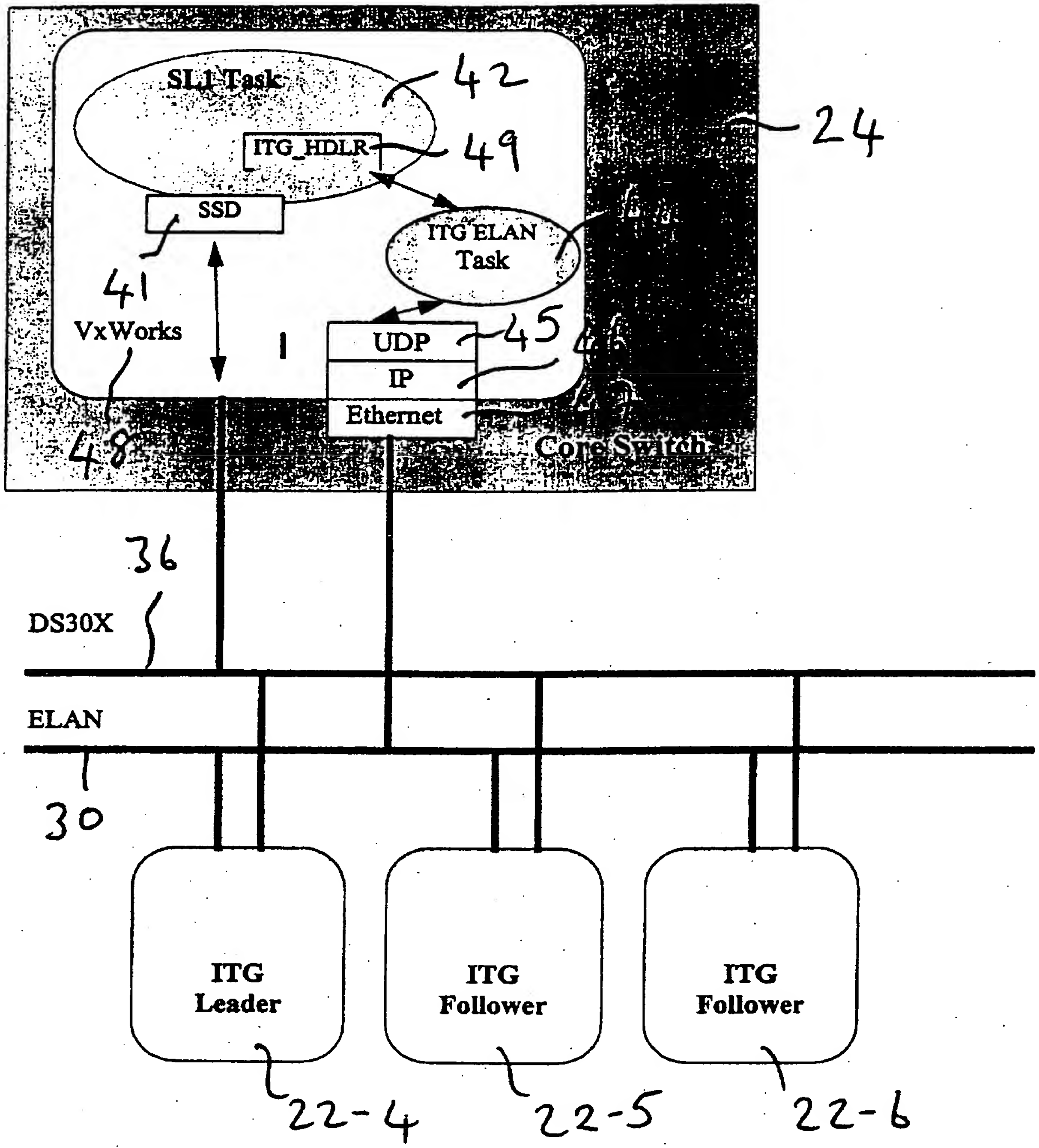

SL1 Task
42
ITG_HDLR
49
24
SSD
ITG ELAN
Task
41
VxWorks
UDP
45
IP
Ethernet
48
Core Switch
36
DS30X
ELAN
30
ITG
Leader
ITG
Follower
ITG
Follower
22-4
22-5
22-6

Fig. 8

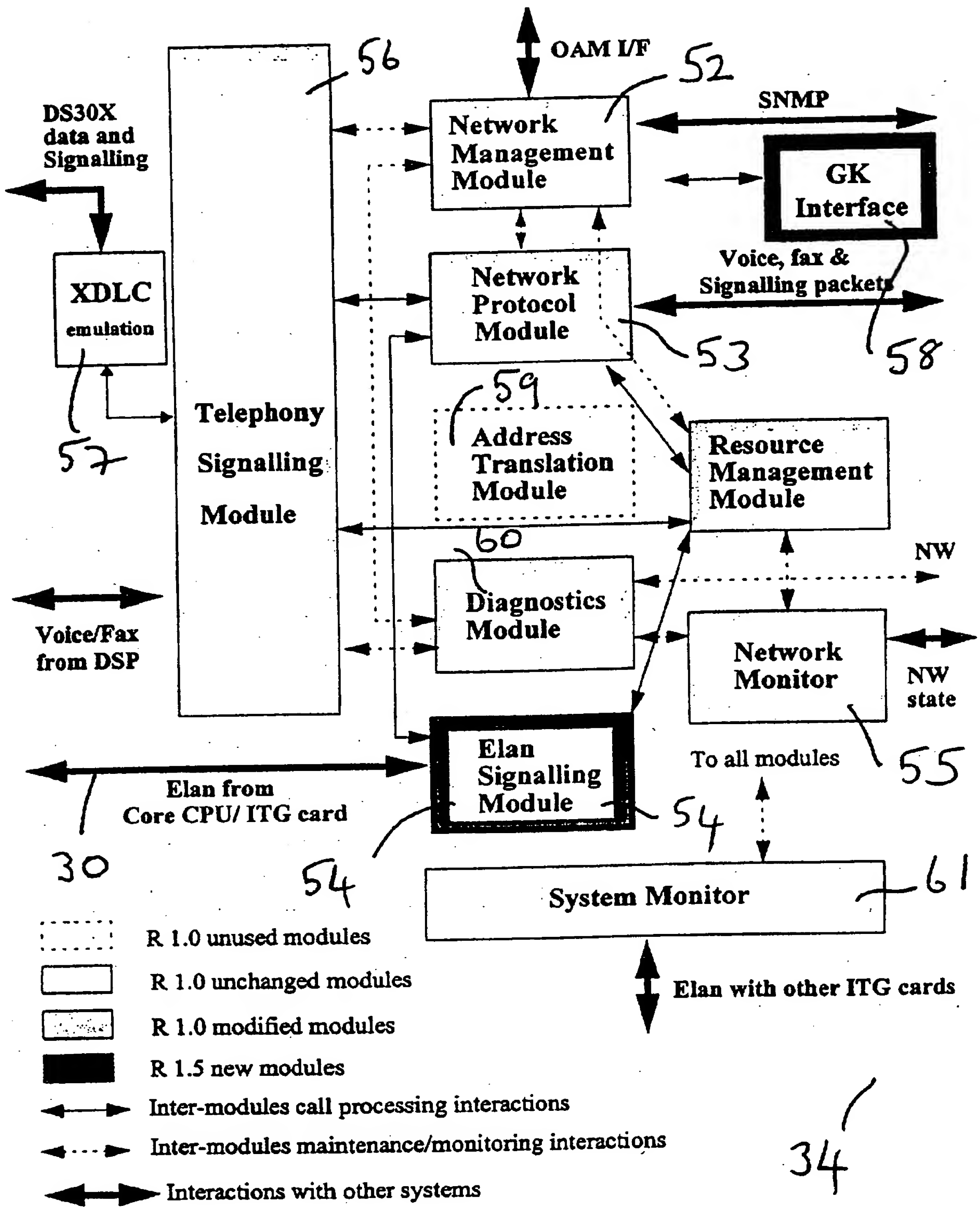

OAM I/F
56
52
SNMP
DS30X
data and
Signalling
Network
Management
Module
GK
Interface
XDLC
emulation
Network
Protocol
Module
Voice, fax &
Signalling packets
53
58
59
Telephony
Signalling
Module
57
Address
Translation
Module
Resource
Management
Module
60
NW
Diagnostics
Module
Voice/Fax
from DSP
Network
Monitor
NW
state
Elan
Signalling
Module
To all modules
55
Elan from
Core CPU/ ITG card
54
30
54
61
System Monitor
Elan with other ITG cards
R 1.0 unused modules
R 1.0 unchanged modules
R 1.0 modified modules
R 1.5 new modules
Inter-modules call processing interactions
Inter-modules maintenance/monitoring interactions
Interactions with other systems
34

Fig. 9

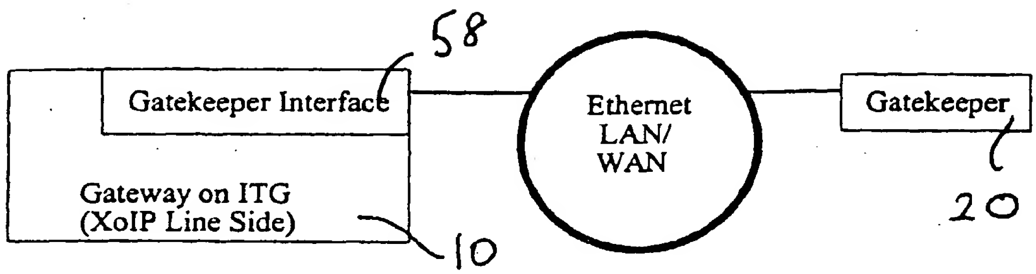

58
Gatekeeper Interface
Gateway on ITG
(XoIP Line Side)
10
Ethernet
LAN/
WAN
Gatekeeper
20

Fig. 10

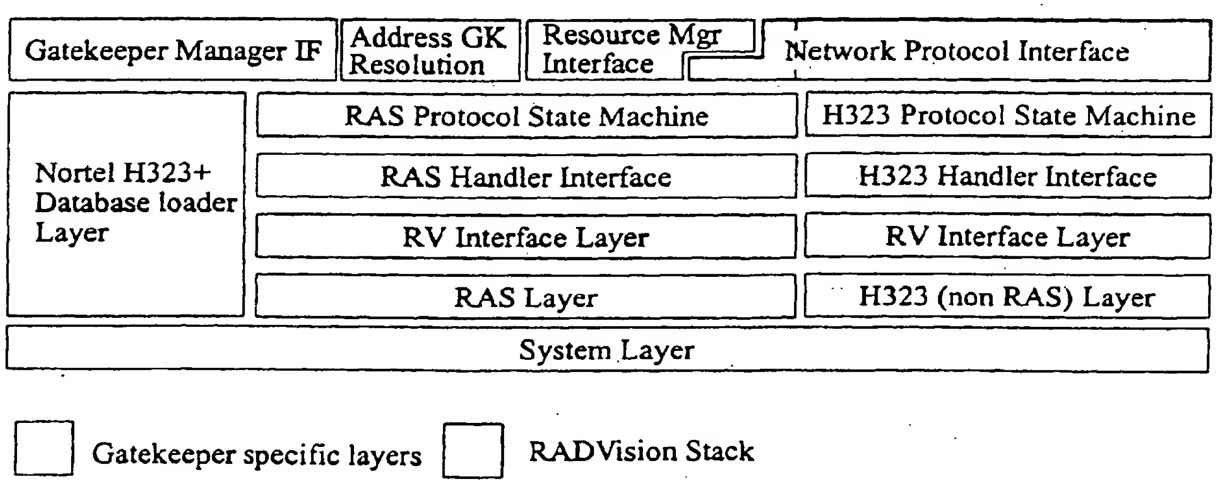

Gatekeeper Manager IF
Address GK Resolution
Resource Mgr Interface
Network Protocol Interface
Nortel H323+ Database loader Layer
RAS Protocol State Machine
H323 Protocol State Machine
RAS Handler Interface
H323 Handler Interface
RV Interface Layer
RV Interface Layer
RAS Layer
H323 (non RAS) Layer
System Layer
Gatekeeper specific layers
RADVision Stack

Fig. 11

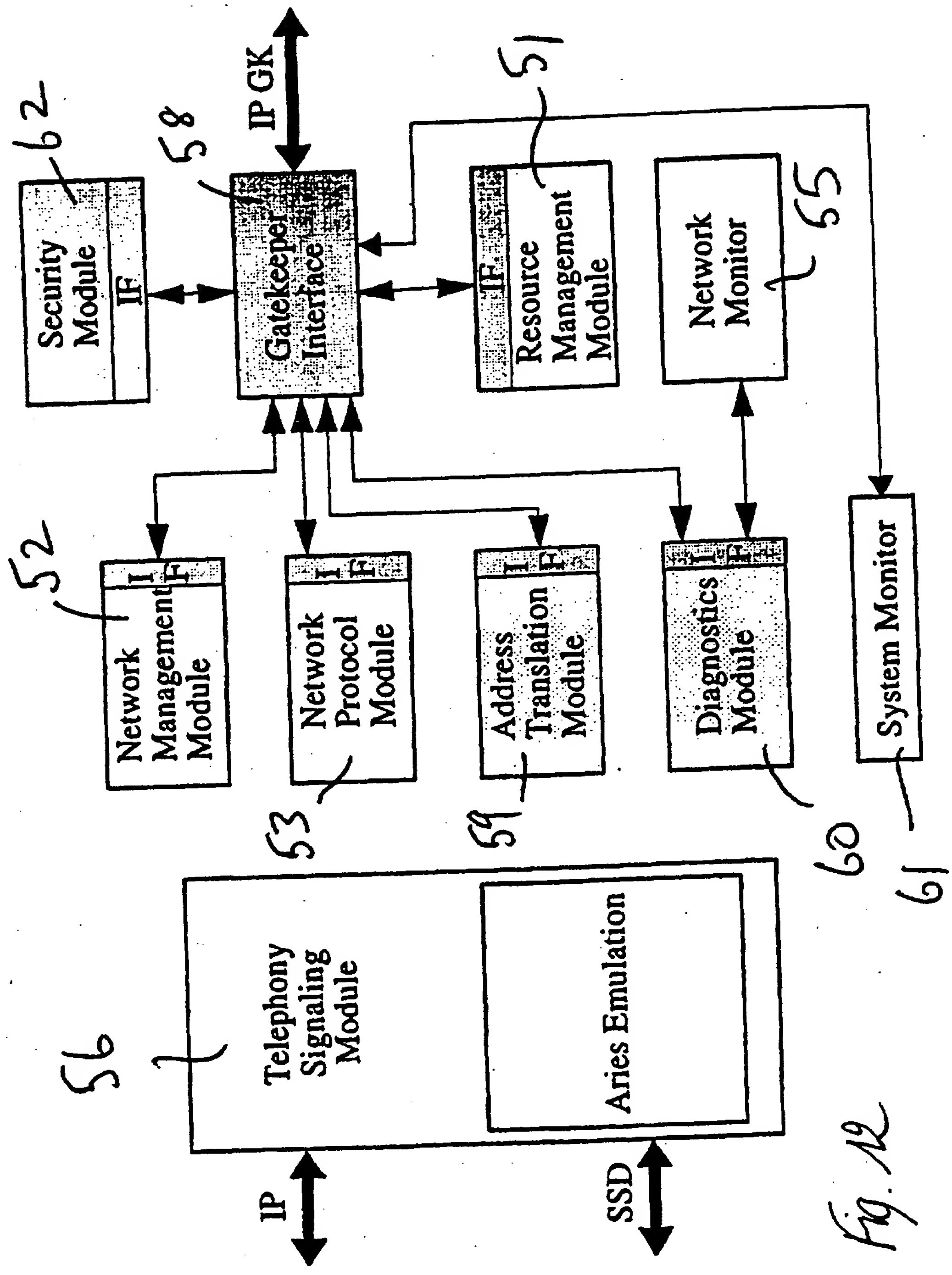

IP GK
Security Module
IF
Gatekeeper Interface
Resource Management Module
Network Monitor
Network Management Module
Network Protocol Module
Address Translation Module
Diagnostics Module
System Monitor
I F
Telephony Signaling Module
Aries Emulation
IP
SSD
62
58
51
55
52
53
59
60
61
56

Fig. 12

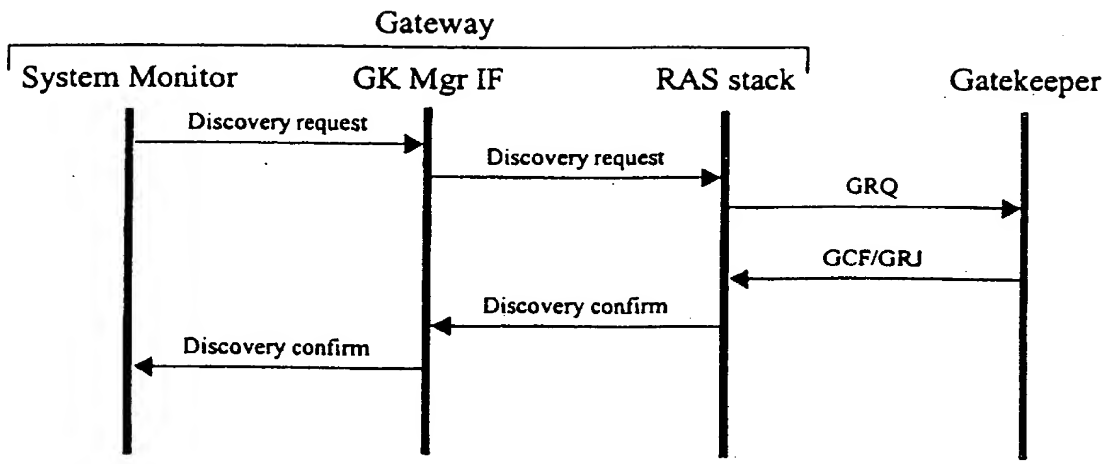

Gateway
System Monitor
GK Mgr IF
RAS stack
Gatekeeper
Discovery request
Discovery request
GRQ
GCF/GRJ
Discovery confirm
Discovery confirm

Fig. 13

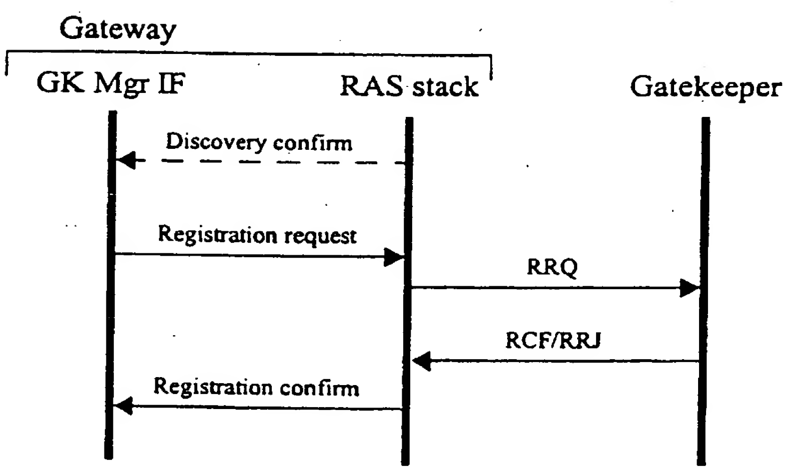

Gateway
GK Mgr IF
RAS stack
Gatekeeper
Discovery confirm
Registration request
RRQ
RCF/RRJ
Registration confirm

Fig. 14

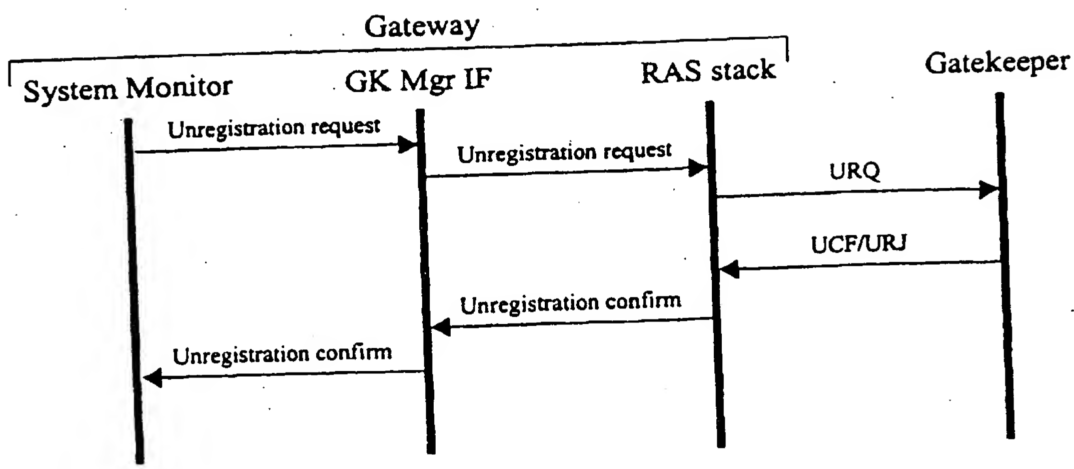

Gateway
System Monitor
GK Mgr IF
RAS stack
Gatekeeper
Unregistration request
Unregistration request
URQ
UCF/URJ
Unregistration confirm
Unregistration confirm

Fig. 15

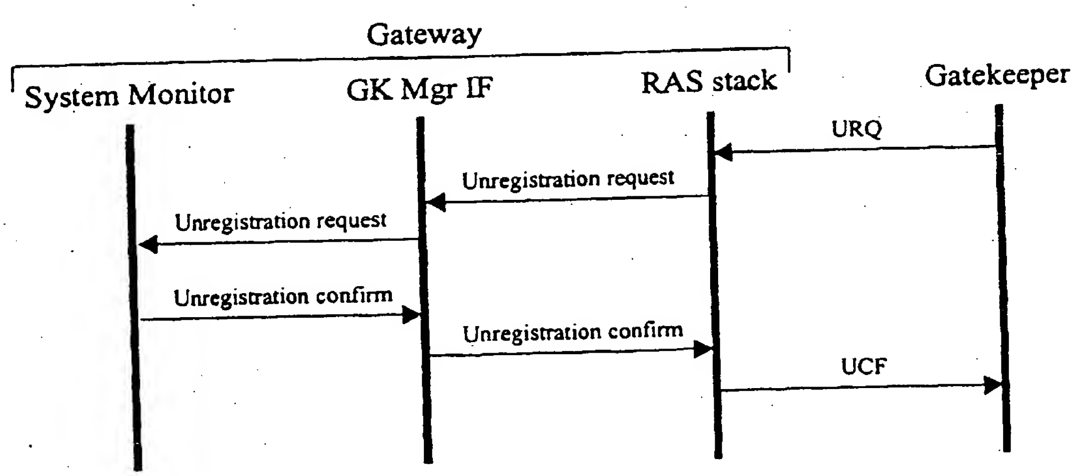

Gateway
System Monitor
GK Mgr IF
RAS stack
Gatekeeper
URQ
Unregistration request
Unregistration request
Unregistration confirm
Unregistration confirm
UCF

Fig. 16

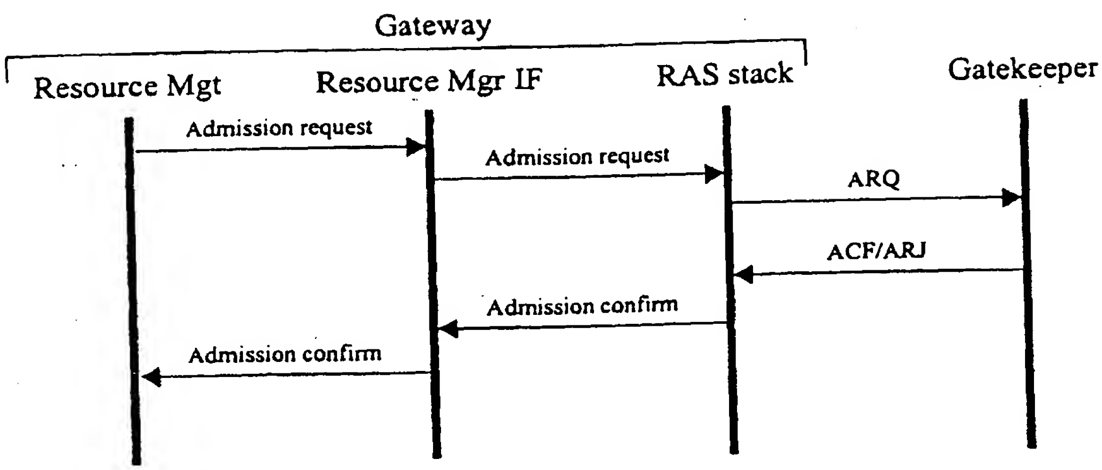

Gateway
Resource Mgt
Resource Mgr IF
RAS stack
Gatekeeper
Admission request
Admission request
ARQ
ACF/ARJ
Admission confirm
Admission confirm

Fig. 17

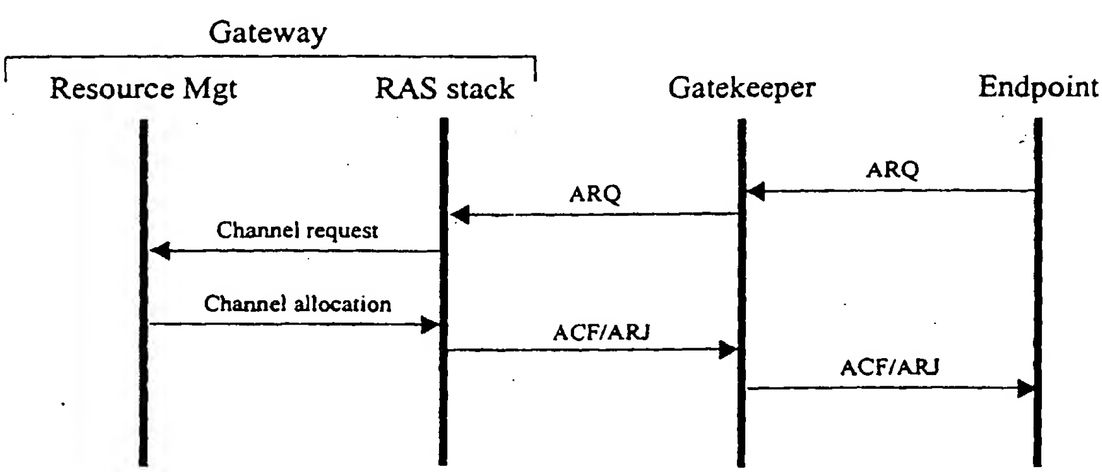

Gateway
Resource Mgt
RAS stack
Gatekeeper
Endpoint
ARQ
ARQ
Channel request
Channel allocation
ACF/ARJ
ACF/ARJ

Fig. 18

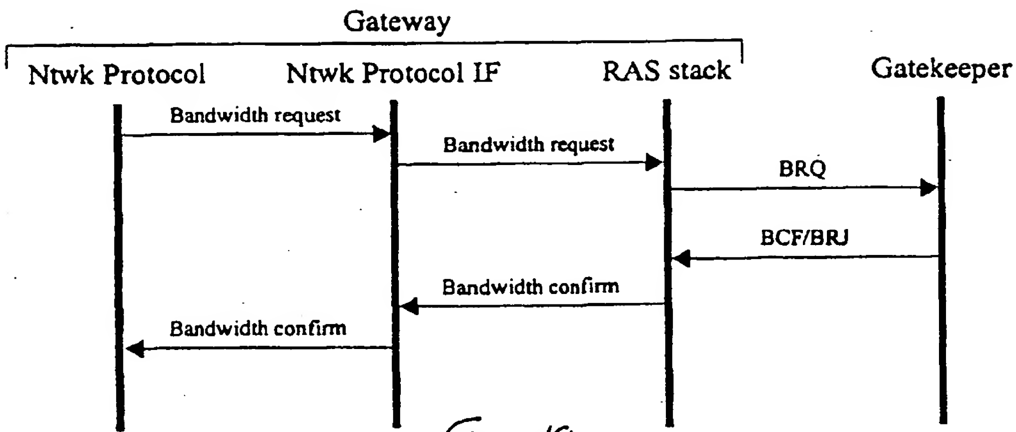


Fig. 19

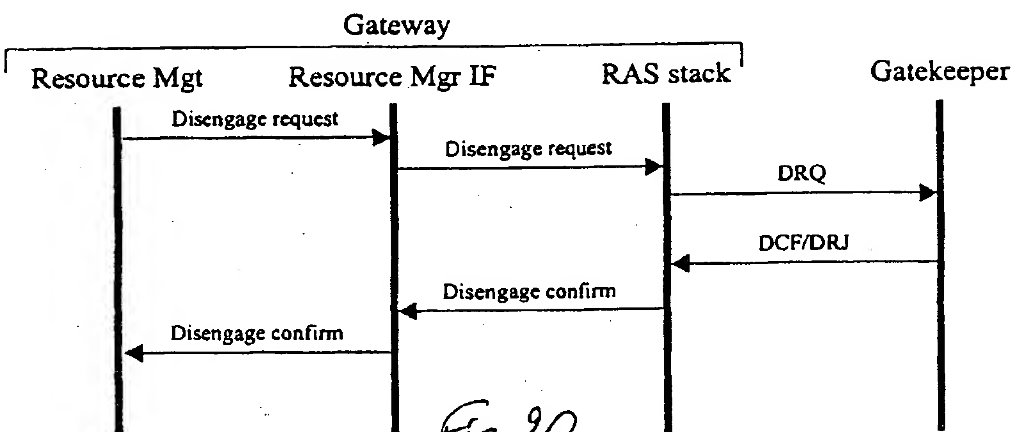


Fig. 20

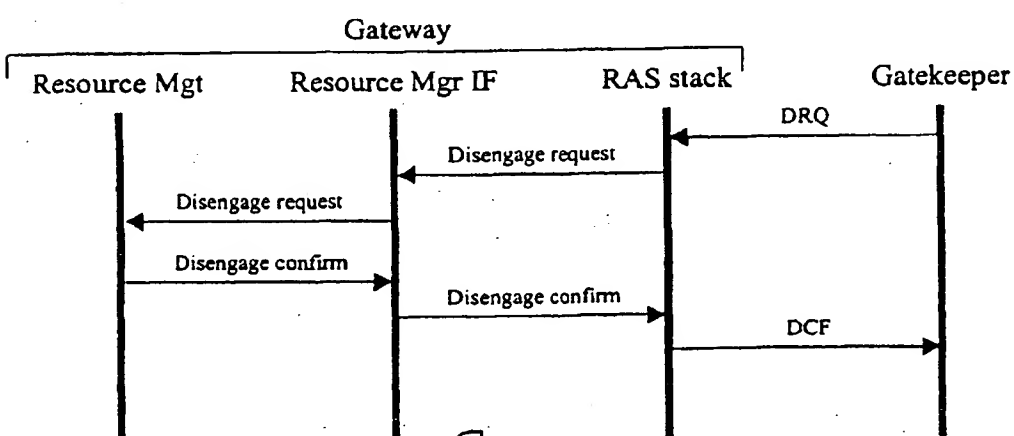


Fig. 21

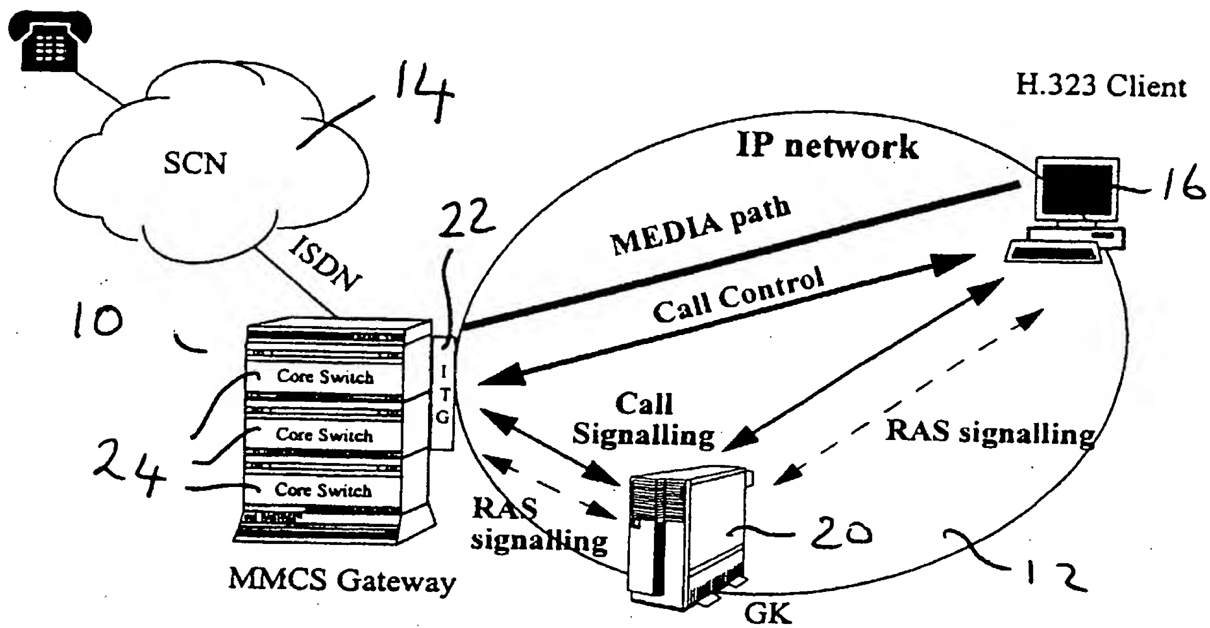

14
SCN
ISDN
10
24
Core Switch
Core Switch
Core Switch
I T G
22
MMCS Gateway
IP network
H.323 Client
16
MEDIA path
Call Control
Call Signalling
RAS signalling
RAS signalling
20
12
GK

Fig. 22

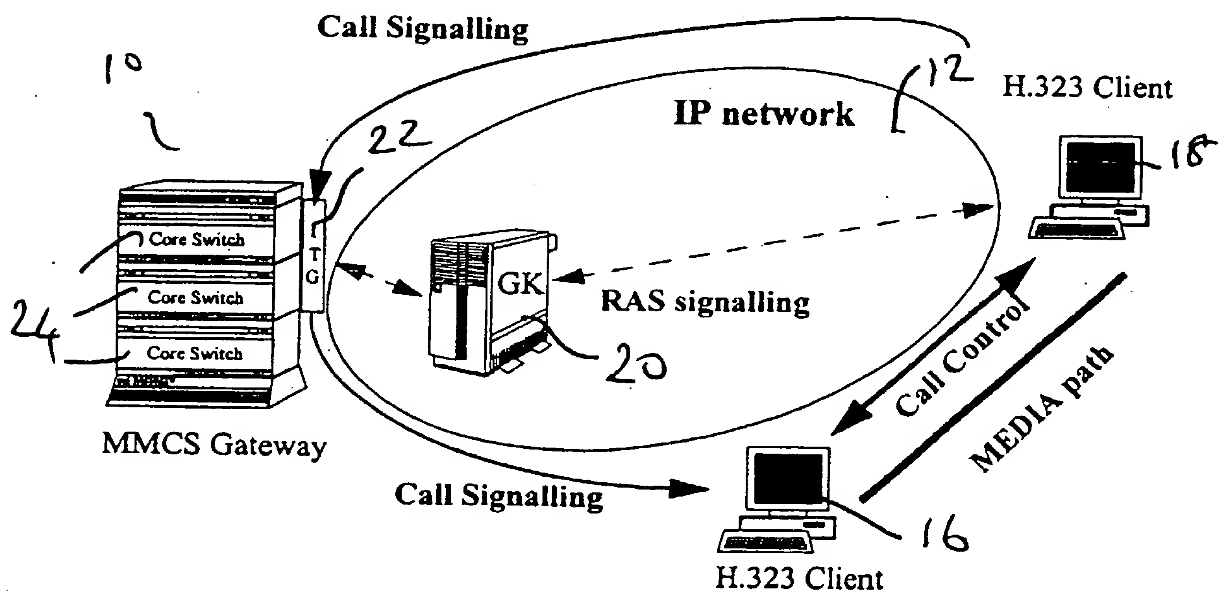
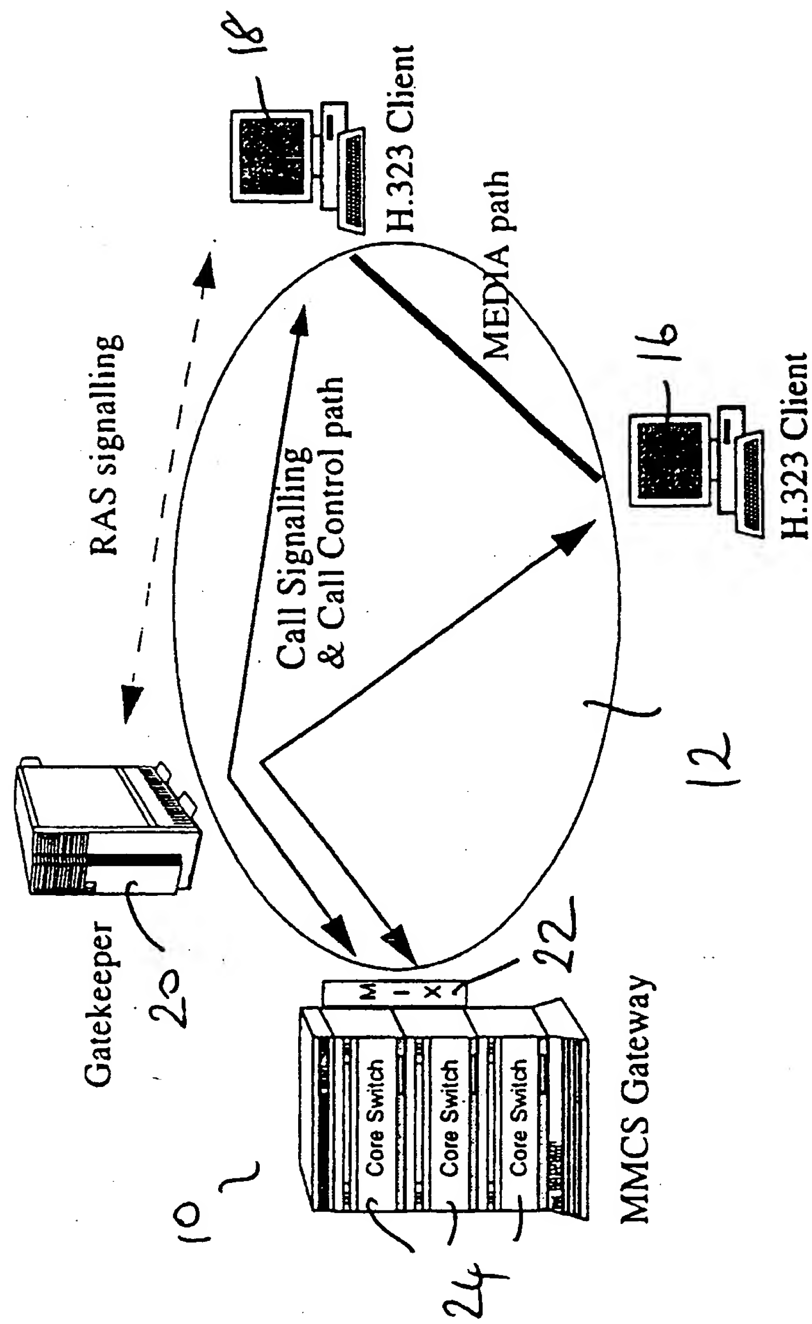
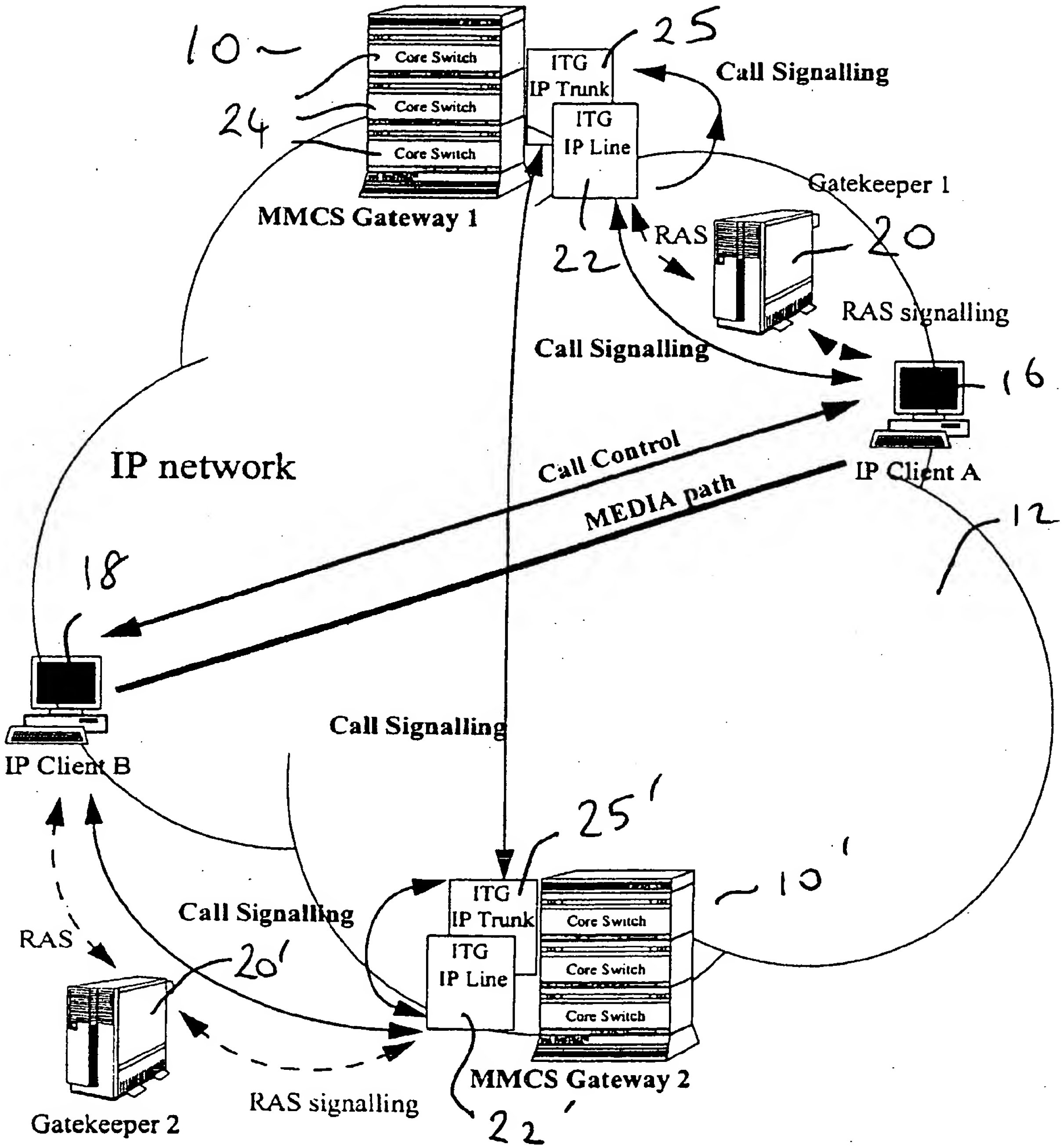

Call Signalling
10
12
H.323 Client
IP network
22
18
Core Switch
Core Switch
Core Switch
I T G
24
GK
RAS signalling
20
Call Control
MEDIA path
MMCS Gateway
Call Signalling
16
H.323 Client

Fig. 24



RAS signalling
Call Signalling
& Call Control path
MEDIA path
H.323 Client
H.323 Client
Gatekeeper
MMCS Gateway
Core Switch
Core Switch
Core Switch
M
I
X
18
16
12
20
22
10
24

Fig. 23



10
24
Core Switch
Core Switch
Core Switch
ITG
IP Trunk
ITG
IP Line
25
Call Signalling
MMCS Gateway 1
22
RAS
Gatekeeper 1
20
RAS signalling
Call Signalling
16
IP Client A
IP network
Call Control
MEDIA path
12
18
IP Client B
Call Signalling
25'
ITG
IP Trunk
ITG
IP Line
10'
Core Switch
Core Switch
Core Switch
RAS
Call Signalling
20'
MMCS Gateway 2
Gatekeeper 2
RAS signalling
22'

Fig. 25

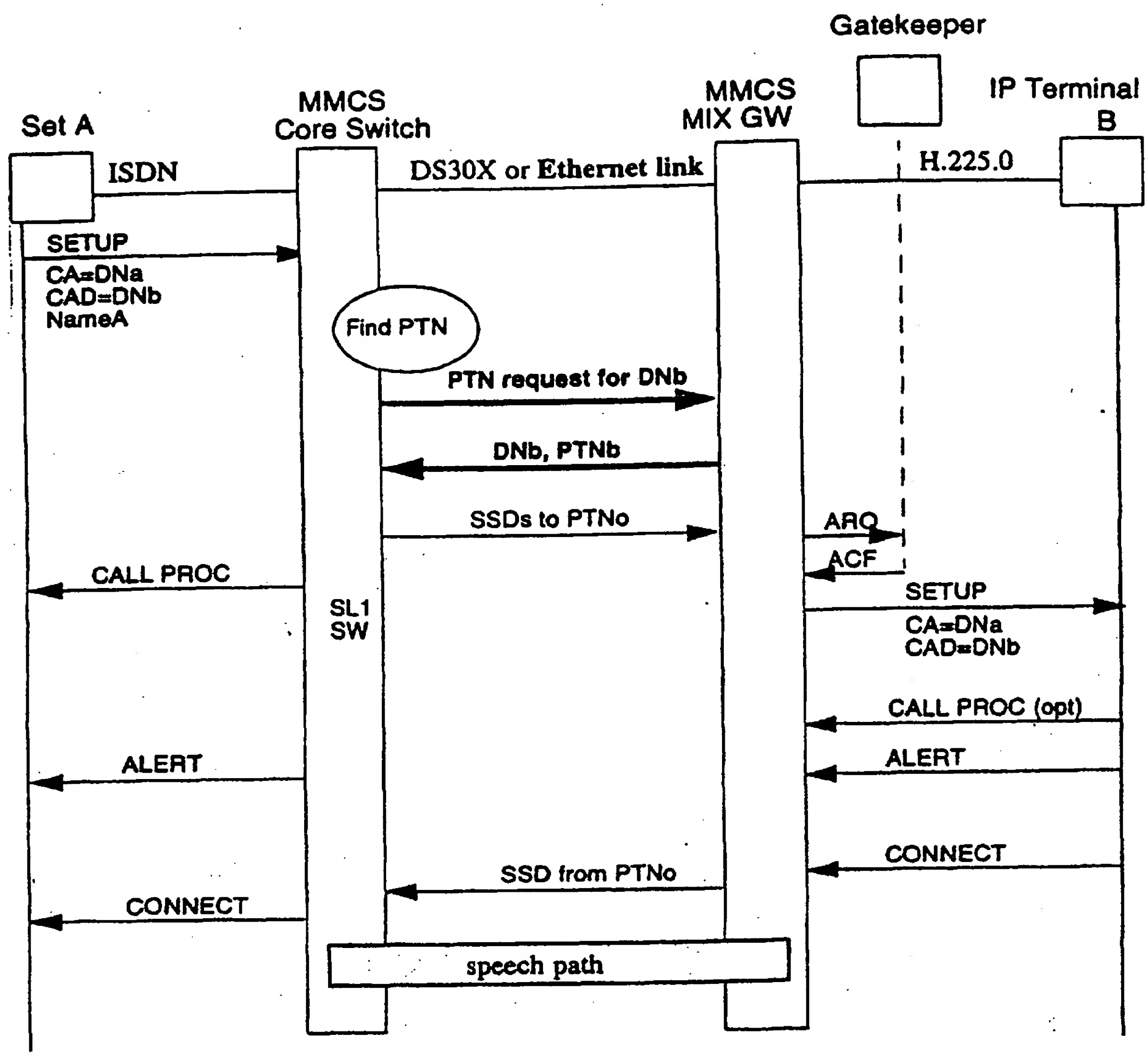

Gatekeeper
Set A
MMCS
Core Switch
MMCS
MIX GW
IP Terminal
B
ISDN
DS30X or Ethernet link
H.225.0
SETUP
CA=DNa
CAD=DNb
NameA
Find PTN
PTN request for DNb
DNb, PTNb
SSDs to PTNo
ARQ
ACF
CALL PROC
SL1
SW
SETUP
CA=DNa
CAD=DNb
CALL PROC (opt)
ALERT
ALERT
CONNECT
SSD from PTNo
CONNECT
speech path

Fig. 26

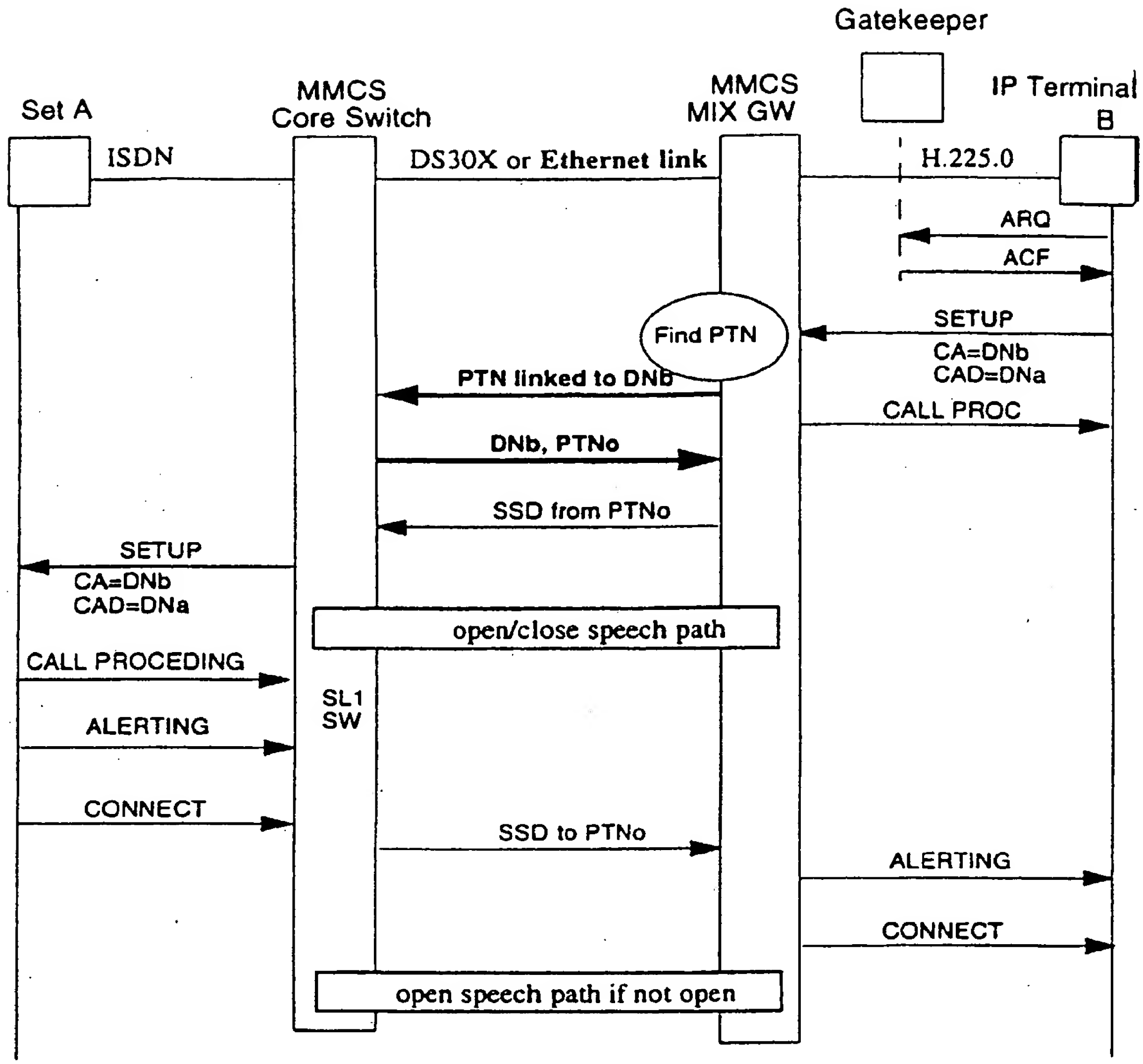

Gatekeeper
Set A
MMCS
Core Switch
MMCS
MIX GW
IP Terminal
B
ISDN
DS30X or Ethernet link
H.225.0
ARQ
ACF
SETUP
CA=DNb
CAD=DNa
Find PTN
PTN linked to DNb
CALL PROC
DNb, PTNo
SSD from PTNo
SETUP
CA=DNb
CAD=DNa
open/close speech path
CALL PROCEDING
SL1
SW
ALERTING
CONNECT
SSD to PTNo
ALERTING
CONNECT
open speech path if not open

Fig. 27

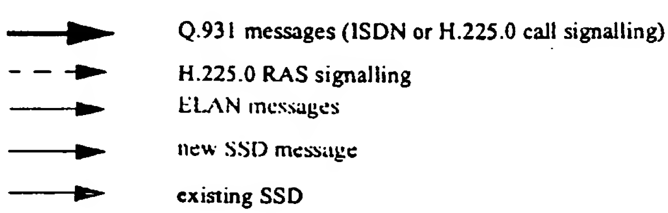

Q.931 messages (ISDN or H.225.0 call signalling)
H.225.0 RAS signalling
ELAN messages
new SSD message
existing SSD

Fig. 28

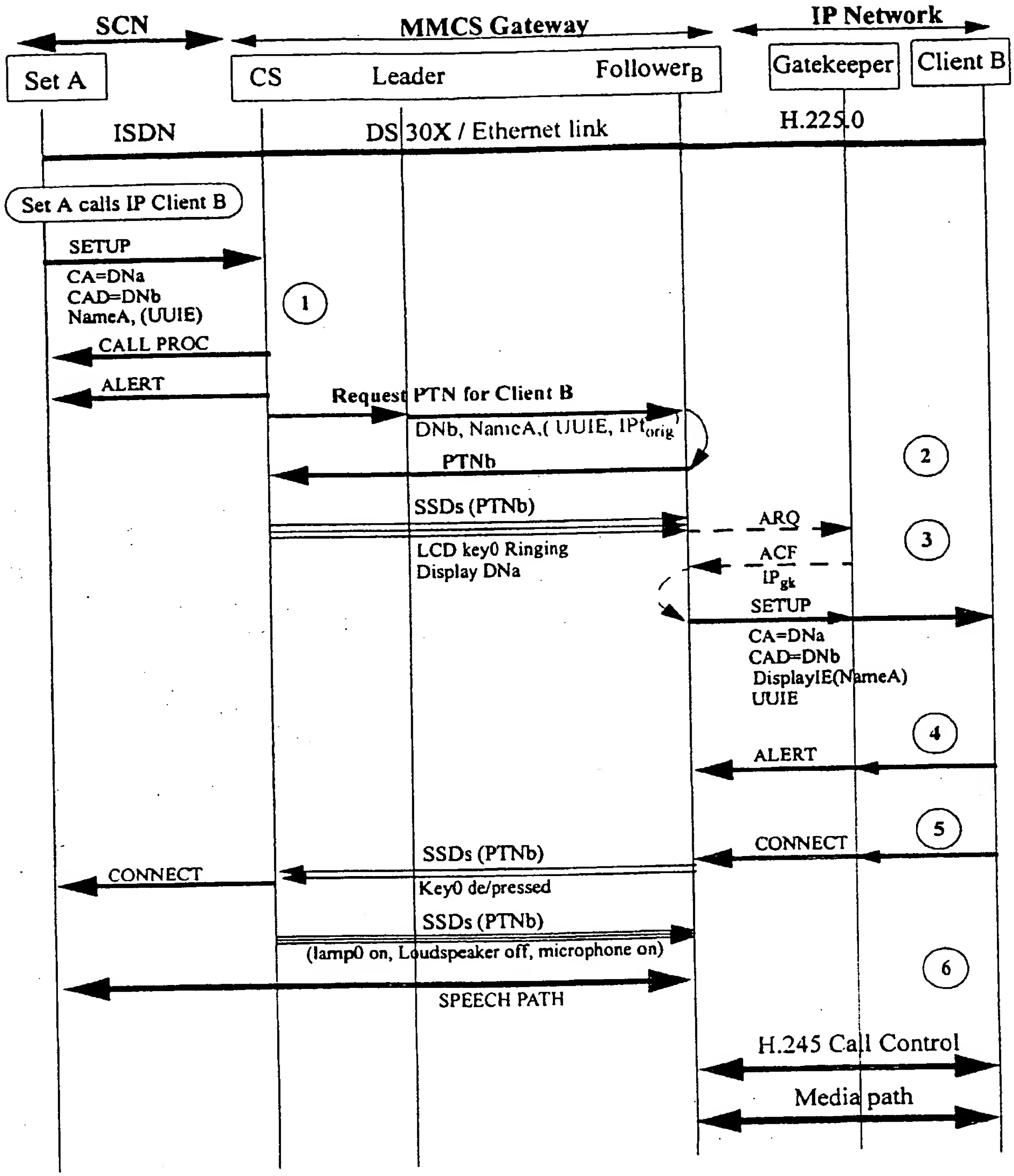

SCN
MMCS Gateway
IP Network
Set A
CS
Leader
Follower$_B$
Gatekeeper
Client B
ISDN
DS 30X / Ethernet link
H.225.0
Set A calls IP Client B
SETUP
CA=DNa
CAD=DNb
NameA, (UUIE)
1
CALL PROC
ALERT
Request PTN for Client B
DNb, NameA,(UUIE, IPt$_{orig}$)
PTNb
2
SSDs (PTNb)
ARQ
3
LCD key0 Ringing
Display DNa
ACF
IP$_{gk}$
SETUP
CA=DNa
CAD=DNb
DisplayIE(NameA)
UUIE
4
ALERT
5
CONNECT
SSDs (PTNb)
CONNECT
Key0 de/pressed
SSDs (PTNb)
(lamp0 on, Loudspeaker off, microphone on)
6
SPEECH PATH
H.245 Call Control
Media path

Fig. 29

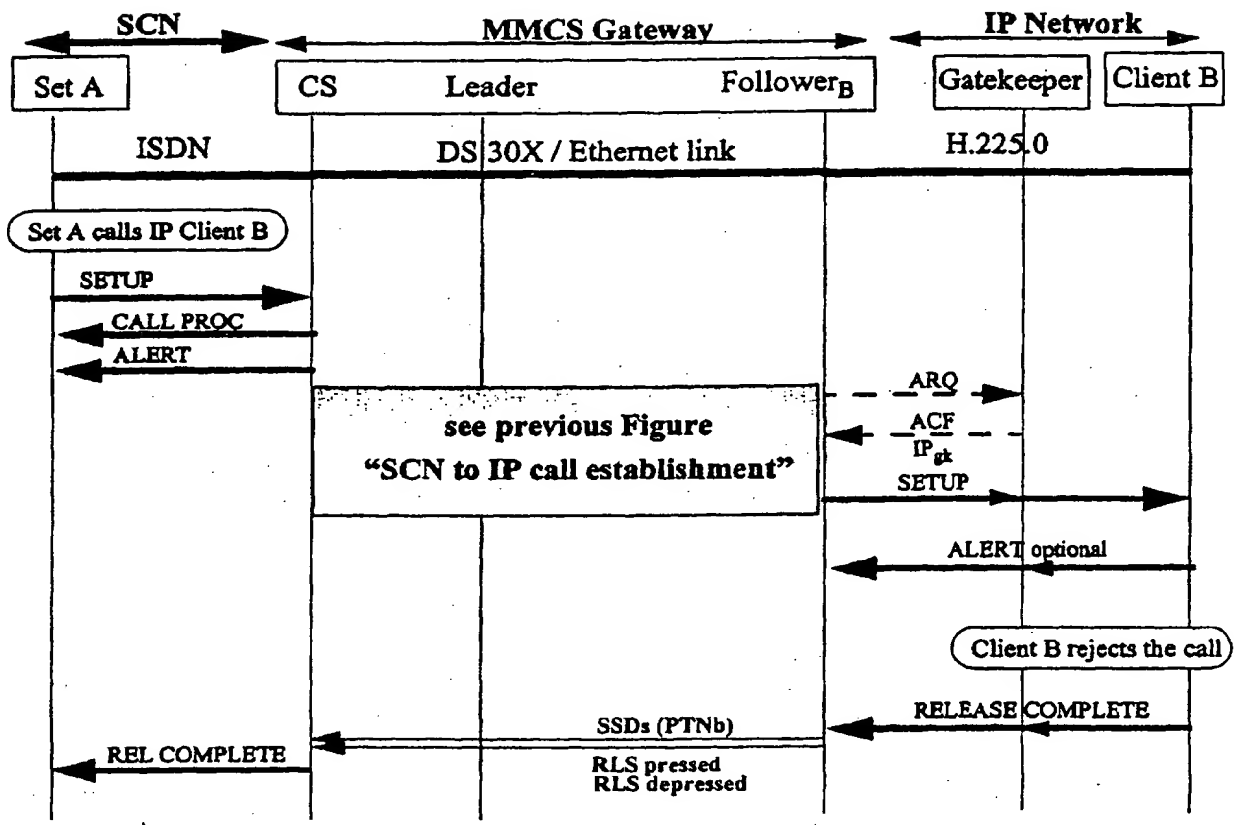

SCN
MMCS Gateway
IP Network
Set A
CS
Leader
Follower$_B$
Gatekeeper
Client B
ISDN
DS 30X / Ethernet link
H.225.0
Set A calls IP Client B
SETUP
CALL PROC
ALERT
ARQ
ACF
IP$_{gk}$
SETUP
see previous Figure
"SCN to IP call establishment"
ALERT optional
Client B rejects the call
RELEASE COMPLETE
SSDs (PTNb)
RLS pressed
RLS depressed
REL COMPLETE

Fig. 30

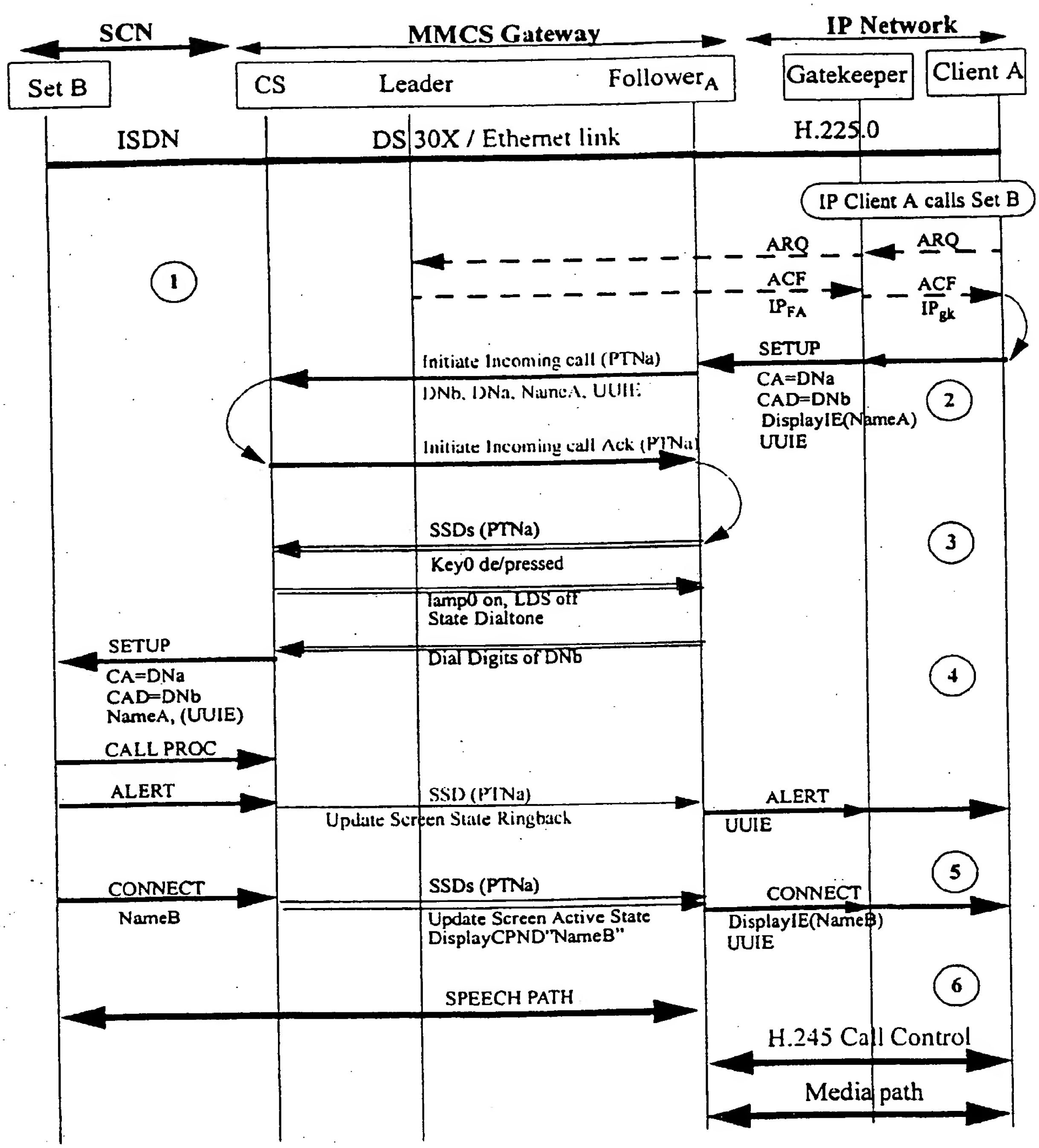

SCN
MMCS Gateway
IP Network
Set B
CS
Leader
FollowerA
Gatekeeper
Client A
ISDN
DS 30X / Ethernet link
H.225.0
IP Client A calls Set B
ARQ
ARQ
ACF
IPFA
ACF
IPgk
1
Initiate Incoming call (PTNa)
DNb, DNa, NameA, UUIE
SETUP
CA=DNa
CAD=DNb
DisplayIE(NameA)
UUIE
2
Initiate Incoming call Ack (PTNa)
SSDs (PTNa)
Key0 de/pressed
3
lamp0 on, LDS off
State Dialtone
Dial Digits of DNb
SETUP
CA=DNa
CAD=DNb
NameA, (UUIE)
4
CALL PROC
ALERT
SSD (PTNa)
Update Screen State Ringback
ALERT
UUIE
CONNECT
NameB
SSDs (PTNa)
Update Screen Active State
DisplayCPND"NameB"
CONNECT
DisplayIE(NameB)
UUIE
5
SPEECH PATH
6
H.245 Call Control
Media path

Fig. 31

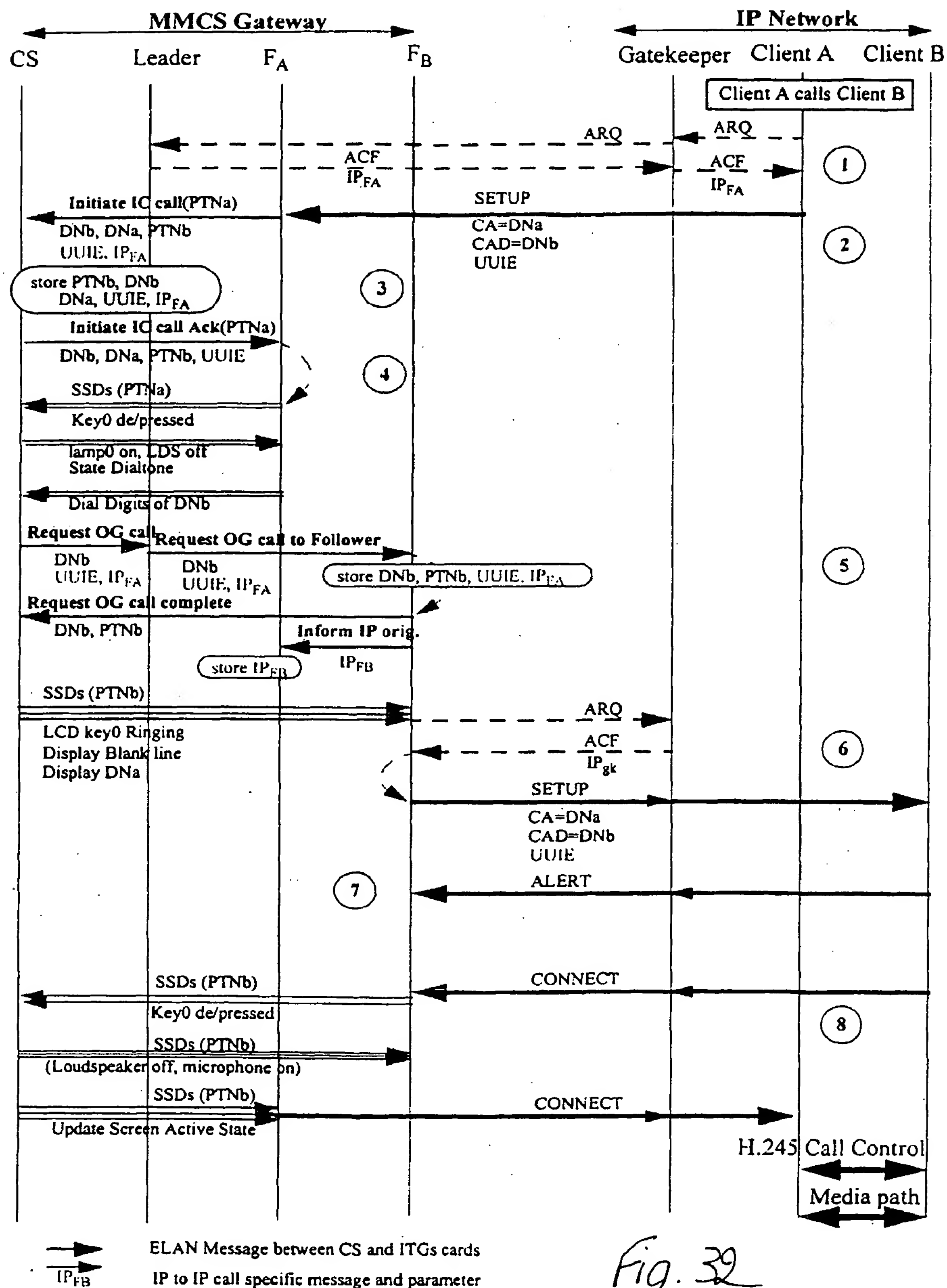

MMCS Gateway
IP Network
CS
Leader
F_A
F_B
Gatekeeper
Client A
Client B
Client A calls Client B
ARQ
ARQ
ACF
IP_{FA}
ACF
IP_{FA}
1
Initiate IC call(PTNa)
DNb, DNa, PTNb
UUIE, IP_{FA}
SETUP
CA=DNa
CAD=DNb
UUIE
2
store PTNb, DNb
DNa, UUIE, IP_{FA}
3
Initiate IC call Ack(PTNa)
DNb, DNa, PTNb, UUIE
4
SSDs (PTNa)
Key0 de/pressed
lamp0 on, LDS off
State Dialtone
Dial Digits of DNb
Request OG call
DNb
UUIE, IP_{FA}
Request OG call to Follower
DNb
UUIE, IP_{FA}
store DNb, PTNb, UUIE, IP_{FA}
5
Request OG call complete
DNb, PTNb
Inform IP orig.
IP_{FB}
store IP_{FB}
SSDs (PTNb)
ARQ
LCD key0 Ringing
Display Blank line
Display DNa
ACF
IP_{gk}
6
SETUP
CA=DNa
CAD=DNb
UUIE
7
ALERT
SSDs (PTNb)
CONNECT
Key0 de/pressed
8
SSDs (PTNb)
(Loudspeaker off, microphone on)
SSDs (PTNb)
CONNECT
Update Screen Active State
H.245 Call Control
Media path
ELAN Message between CS and ITGs cards
IP_{FB}
IP to IP call specific message and parameter

Fig. 32

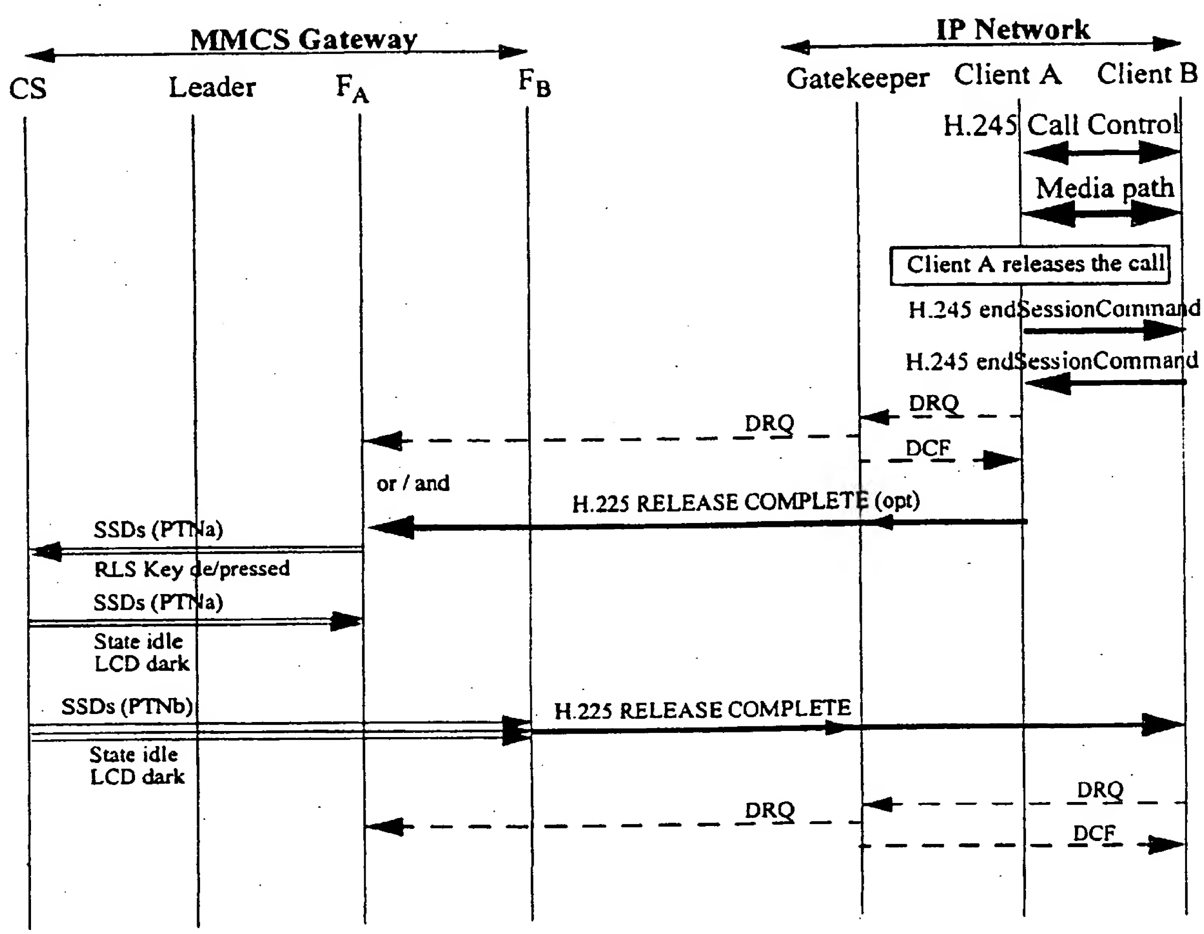

MMCS Gateway
IP Network
CS
Leader
F_A
F_B
Gatekeeper
Client A
Client B
H.245 Call Control
Media path
Client A releases the call
H.245 endSessionCommand
H.245 endSessionCommand
DRQ
DRQ
DCF
or / and
H.225 RELEASE COMPLETE (opt)
SSDs (PTNa)
RLS Key de/pressed
SSDs (PTNa)
State idle
LCD dark
SSDs (PTNb)
H.225 RELEASE COMPLETE
State idle
LCD dark
DRQ
DRQ
DCF

Fig. 33

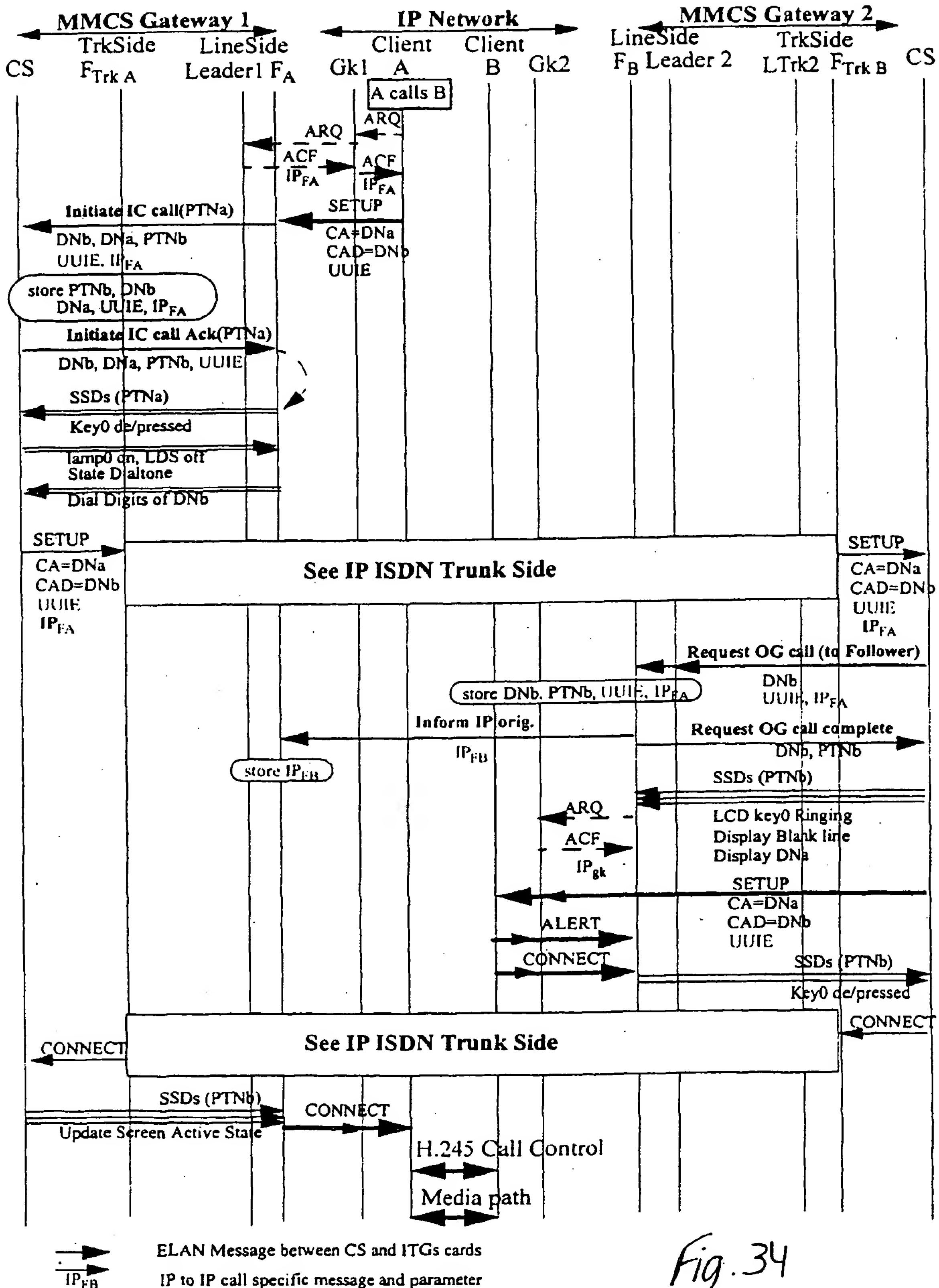

MMCS Gateway 1
TrkSide
LineSide
CS
FTrk A
Leader1 FA
IP Network
Client A
Client B
Gk1
Gk2
MMCS Gateway 2
LineSide
FB Leader 2
TrkSide
LTrk2 FTrk B
CS
A calls B
ARQ
ACF
IPFA
SETUP
CA=DNa
CAD=DNb
UUIE
Initiate IC call(PTNa)
DNb, DNa, PTNb
UUIE, IPFA
store PTNb, DNb
DNa, UUIE, IPFA
Initiate IC call Ack(PTNa)
DNb, DNa, PTNb, UUIE
SSDs (PTNa)
Key0 de/pressed
lamp0 on, LDS off
State Dialtone
Dial Digits of DNb
SETUP
CA=DNa
CAD=DNb
UUIE
IPFA
See IP ISDN Trunk Side
Request OG call (to Follower)
DNb
UUIE, IPFA
store DNb, PTNb, UUIE, IPFA
Inform IP orig.
IPFB
Request OG call complete
DNb, PTNb
store IPFB
SSDs (PTNb)
ARQ
ACF
IPgk
LCD key0 Ringing
Display Blank line
Display DNa
SETUP
CA=DNa
CAD=DNb
UUIE
ALERT
CONNECT
SSDs (PTNb)
Key0 de/pressed
CONNECT
See IP ISDN Trunk Side
CONNECT
SSDs (PTNb)
CONNECT
Update Screen Active State
H.245 Call Control
Media path
ELAN Message between CS and ITGs cards
IPFB
IP to IP call specific message and parameter

Fig. 34

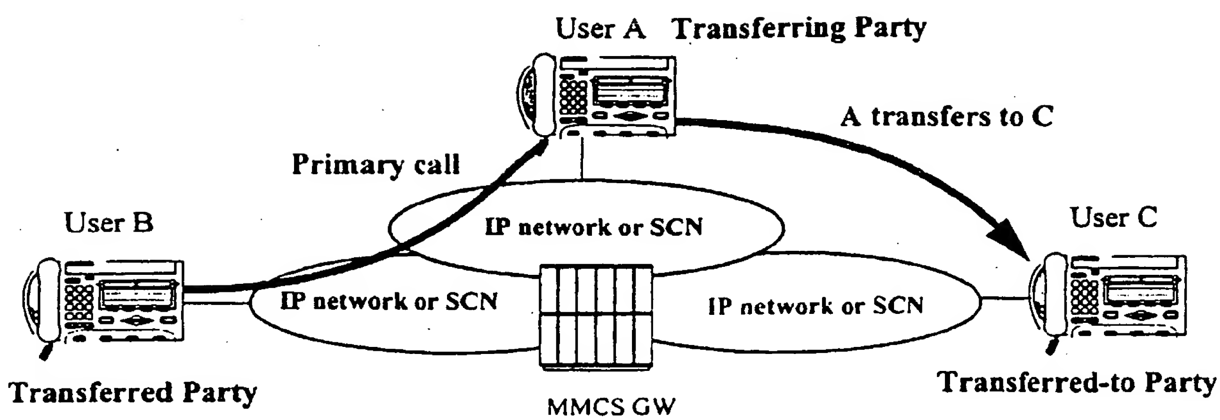


Fig. 35

	Q.931 messages (ISDN or H.225.0 call signalling)
	ELAN messages dedicated to Call Transfer operation
	SSD messages
	H.225.0 RAS signalling
xxx.inv	invoke PDU for operation xxx
xxx.rr	return result PDU for operation xxx
xxx.re	return error PDU for operation xxx
F_{X2}	Follower Card which handles the IP call to Client X. This call is the **secondary** call of the call transfer operation
L	Leader Card
rrNb	rerouting Number
XingNb	transferring Number

Fig. 36

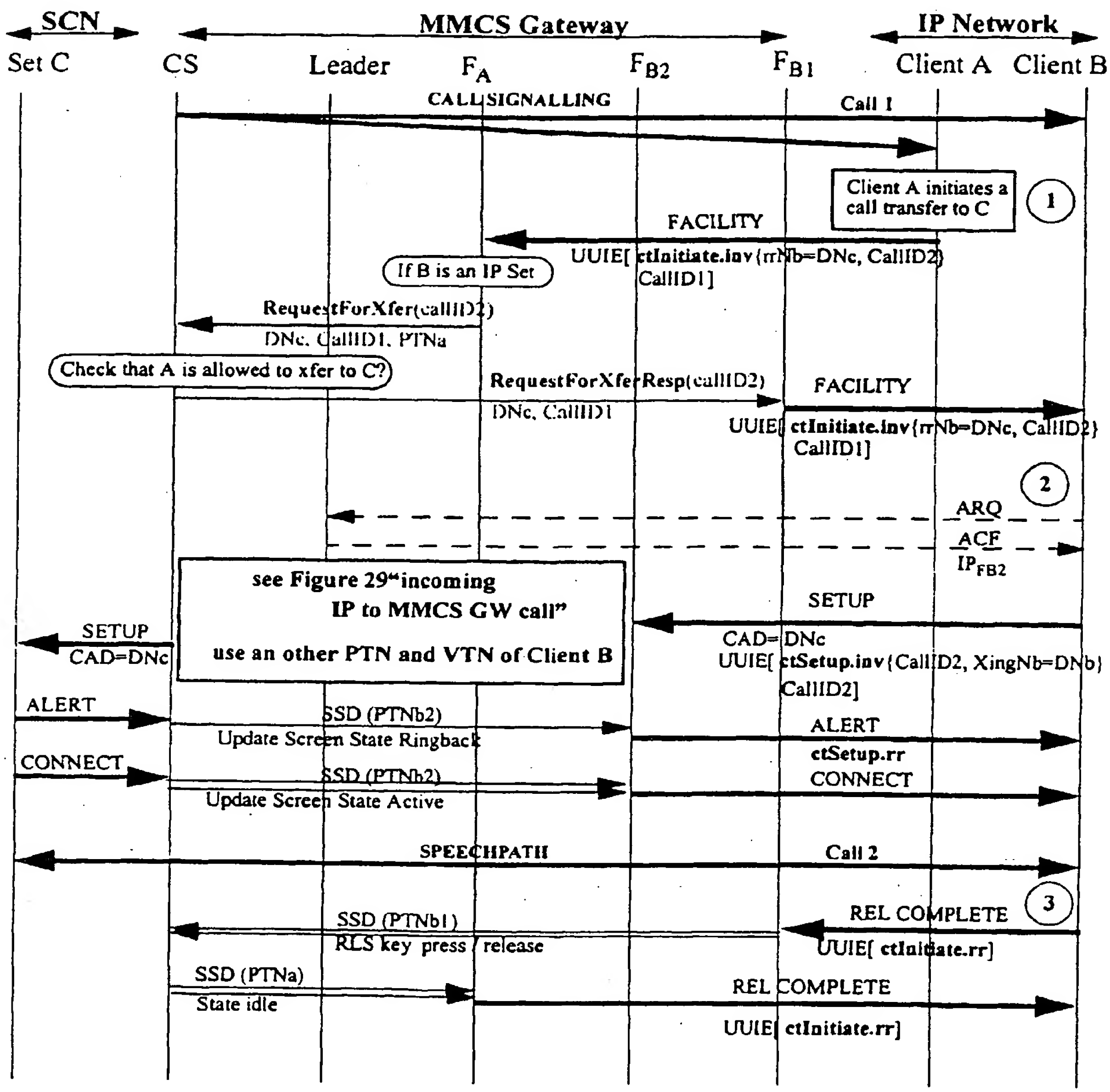

SCN
MMCS Gateway
IP Network
Set C
CS
Leader
FA
FB2
FB1
Client A
Client B
CALL SIGNALLING
Call 1
Client A initiates a call transfer to C
1
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2}
CallID1]
If B is an IP Set
RequestForXfer(callID2)
DNc. CallID1. PTNa
Check that A is allowed to xfer to C?
RequestForXferResp(callID2)
DNc. CallID1
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2}
CallID1]
2
ARQ
ACF
IPFB2
see Figure 29 "incoming IP to MMCS GW call"
use an other PTN and VTN of Client B
SETUP
CAD=DNc
SETUP
CAD=DNc
UUIE[ctSetup.inv{CallID2, XingNb=DNb}
CallID2]
ALERT
SSD (PTNb2)
Update Screen State Ringback
ALERT
ctSetup.rr
CONNECT
SSD (PTNb2)
Update Screen State Active
CONNECT
SPEECHPATH
Call 2
3
REL COMPLETE
SSD (PTNb1)
RLS key press / release
UUIE[ctInitiate.rr]
SSD (PTNa)
State idle
REL COMPLETE
UUIE[ctInitiate.rr]

Fig. 37

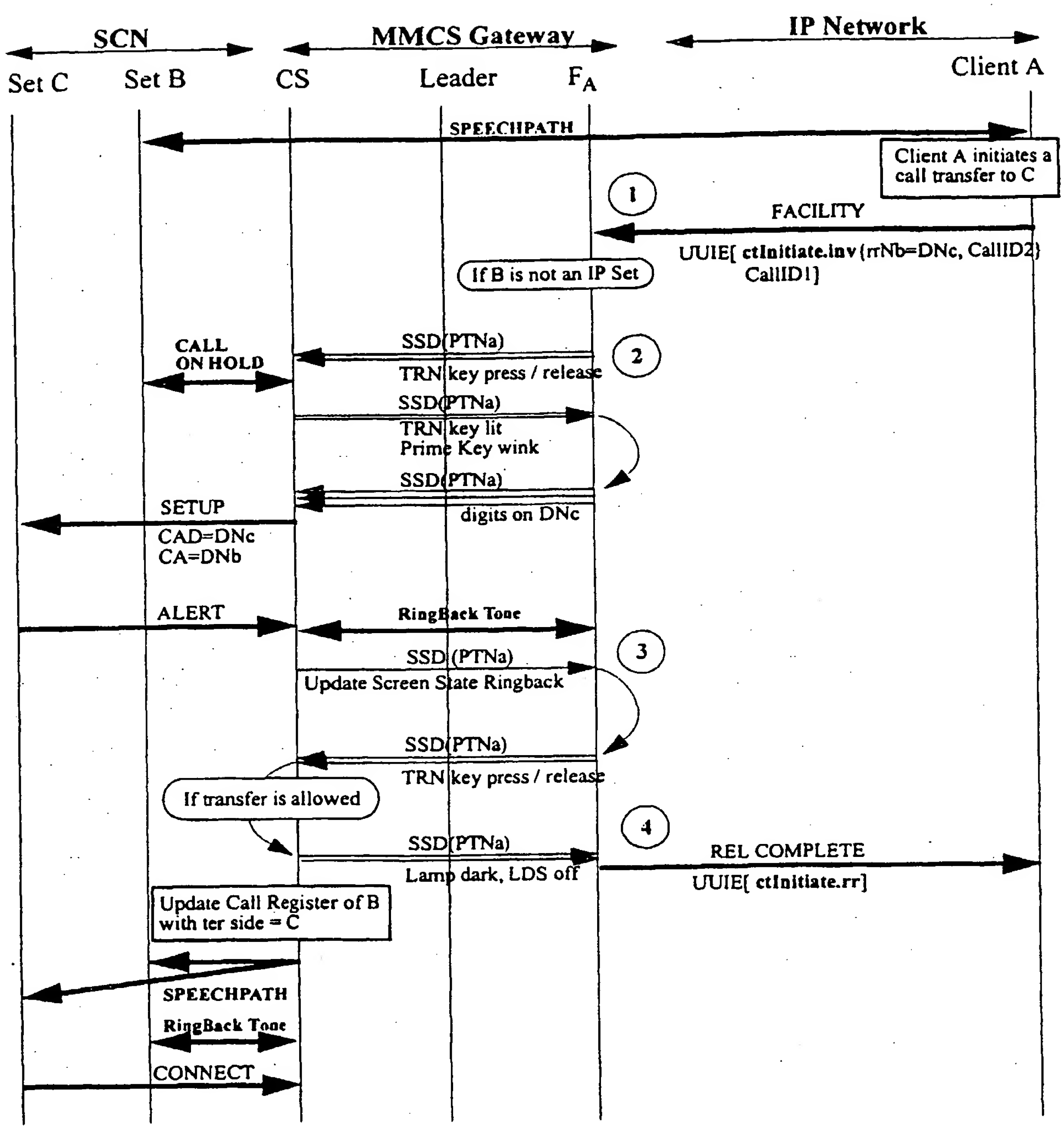

SCN
MMCS Gateway
IP Network
Set C
Set B
CS
Leader
F_A
Client A
SPEECHPATH
Client A initiates a call transfer to C
1
FACILITY
UUIE[ctInitiate.inv (rrNb=DNc, CallID2) CallID1]
If B is not an IP Set
SSD(PTNa)
CALL ON HOLD
2
TRN key press / release
SSD(PTNa)
TRN key lit
Prime Key wink
SSD(PTNa)
SETUP
digits on DNc
CAD=DNc
CA=DNb
ALERT
RingBack Tone
3
SSD (PTNa)
Update Screen State Ringback
SSD(PTNa)
TRN key press / release
If transfer is allowed
4
SSD(PTNa)
REL COMPLETE
Lamp dark, LDS off
UUIE[ctInitiate.rr]
Update Call Register of B with ter side = C
SPEECHPATH
RingBack Tone
CONNECT

Fig. 38

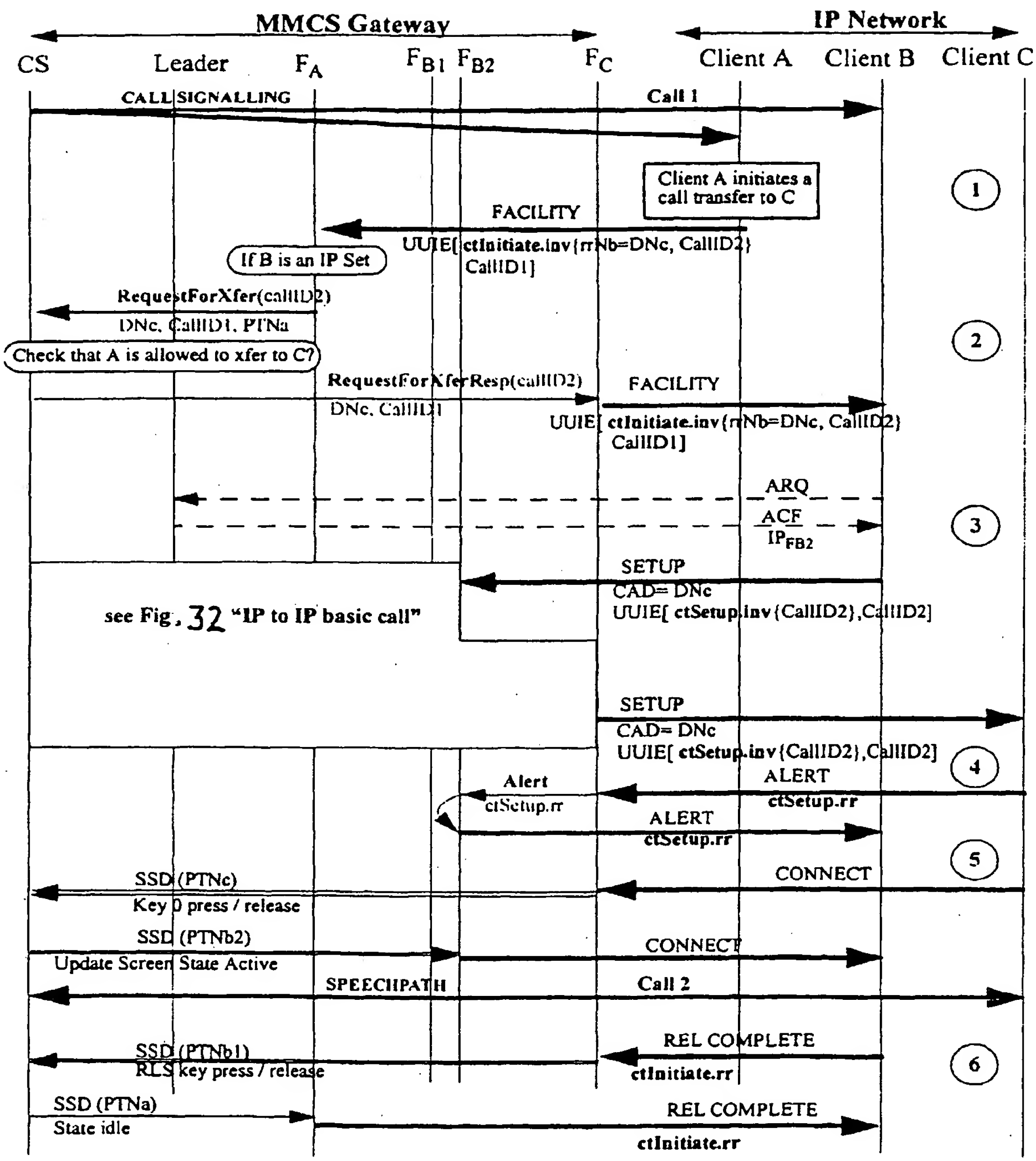
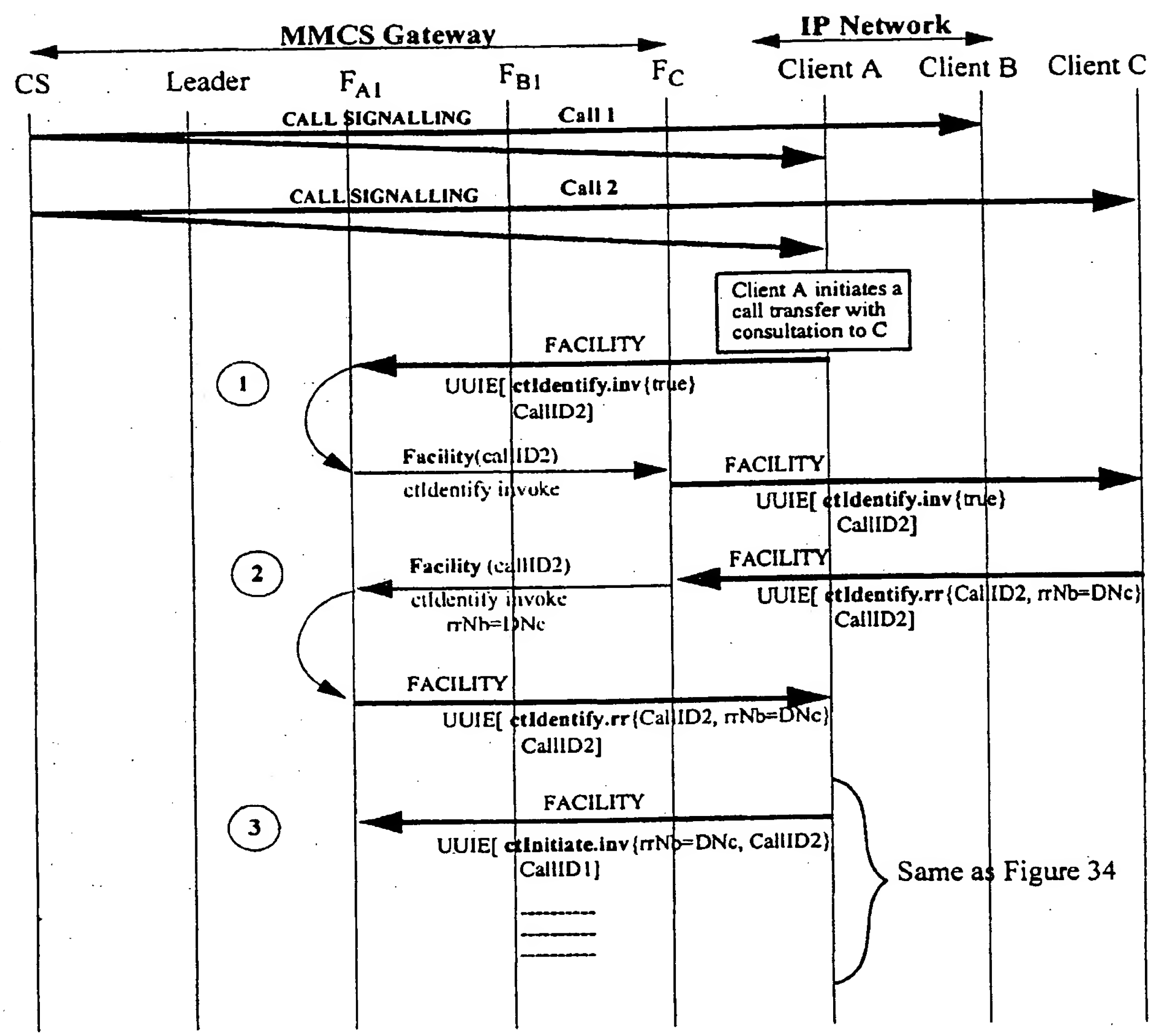

MMCS Gateway
IP Network
CS
Leader
F_A
F_{B1}
F_{B2}
F_C
Client A
Client B
Client C
CALL SIGNALLING
Call 1
Client A initiates a call transfer to C
1
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2}
CallID1]
If B is an IP Set
RequestForXfer(callID2)
DNc, CallID1, PTNa
2
Check that A is allowed to xfer to C?
RequestForXferResp(callID2)
DNc, CallID1
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2}
CallID1]
ARQ
ACF
IP_{FB2}
3
SETUP
CAD= DNc
UUIE[ctSetup.inv{CallID2},CallID2]
see Fig. 32 "IP to IP basic call"
SETUP
CAD= DNc
UUIE[ctSetup.inv{CallID2},CallID2]
4
ALERT
ctSetup.rr
Alert
ctSetup.rr
ALERT
ctSetup.rr
5
SSD (PTNc)
Key 0 press / release
CONNECT
SSD (PTNb2)
Update Screen State Active
CONNECT
SPEECHPATH
Call 2
REL COMPLETE
SSD (PTNb1)
RLS key press / release
ctInitiate.rr
6
SSD (PTNa)
State idle
REL COMPLETE
ctInitiate.rr

Fig. 39



MMCS Gateway
IP Network
CS
Leader
F_{A1}
F_{B1}
F_C
Client A
Client B
Client C
CALL SIGNALLING
Call 1
CALL SIGNALLING
Call 2
Client A initiates a call transfer with consultation to C
FACILITY
1
UUIE[ctIdentify.inv{true} CallID2]
Facility(callID2)
ctIdentify invoke
FACILITY
UUIE[ctIdentify.inv{true} CallID2]
2
Facility (callID2)
ctIdentify invoke
rrNb=DNc
FACILITY
UUIE[ctIdentify.rr{CallID2, rrNb=DNc} CallID2]
FACILITY
UUIE[ctIdentify.rr{CallID2, rrNb=DNc} CallID2]
3
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2} CallID1]
Same as Figure 34

Fig. 40

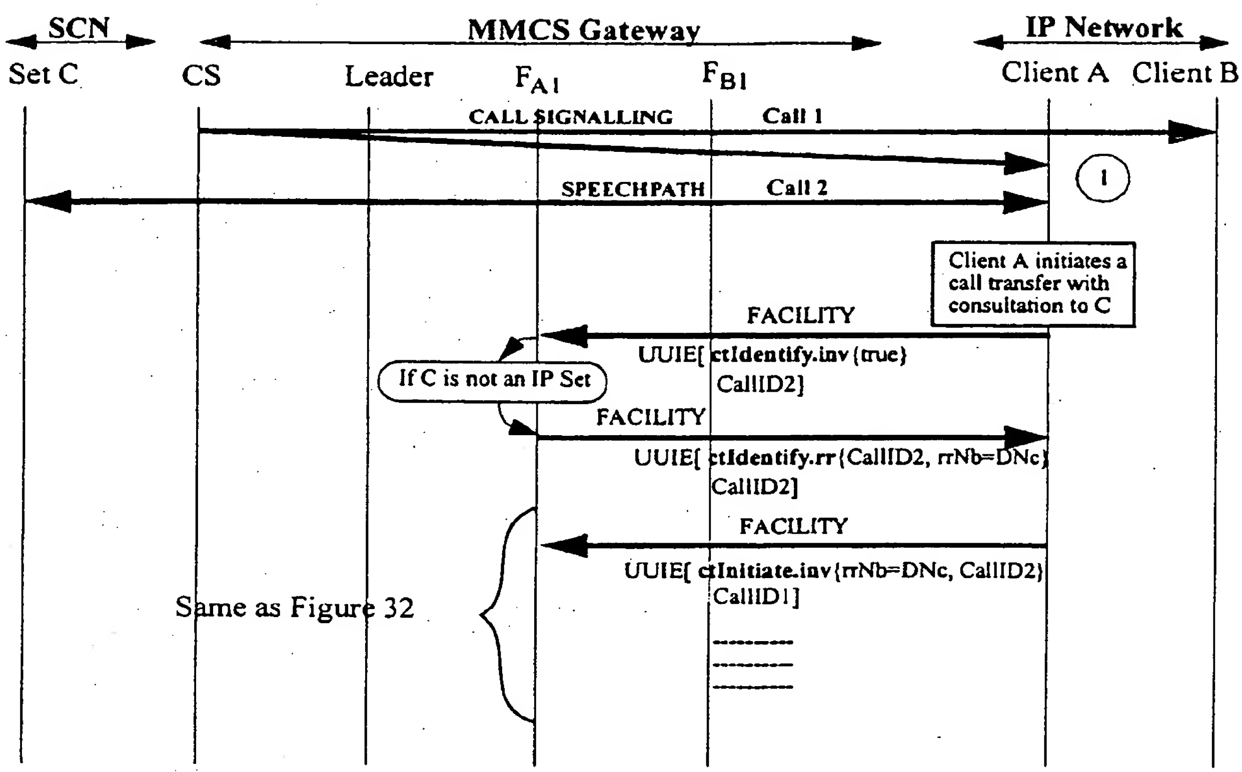

SCN
MMCS Gateway
IP Network
Set C
CS
Leader
F_{A1}
F_{B1}
Client A
Client B
CALL SIGNALLING
Call 1
SPEECHPATH
Call 2
1
Client A initiates a call transfer with consultation to C
FACILITY
UUIE[ctIdentify.inv{true}
CallID2]
If C is not an IP Set
FACILITY
UUIE[ctIdentify.rr{CallID2, rrNb=DNc}
CallID2]
FACILITY
UUIE[ctInitiate.inv{rrNb=DNc, CallID2}
CallID1]
Same as Figure 32

Fig. 41

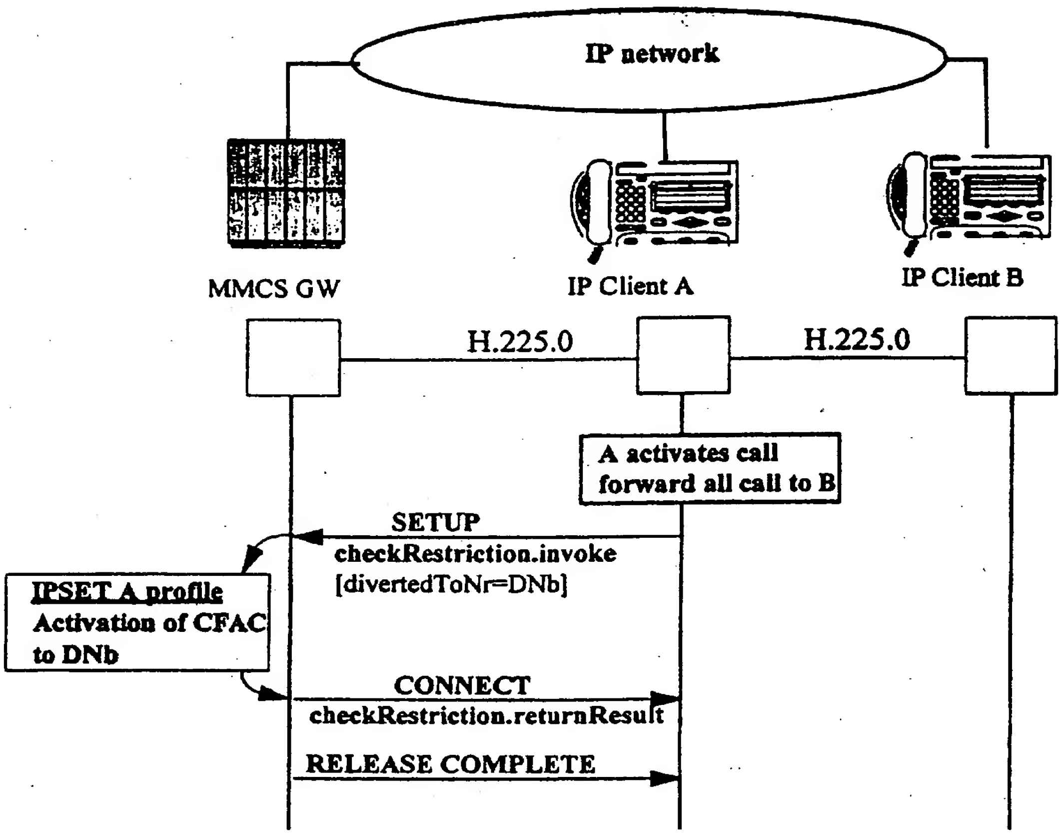
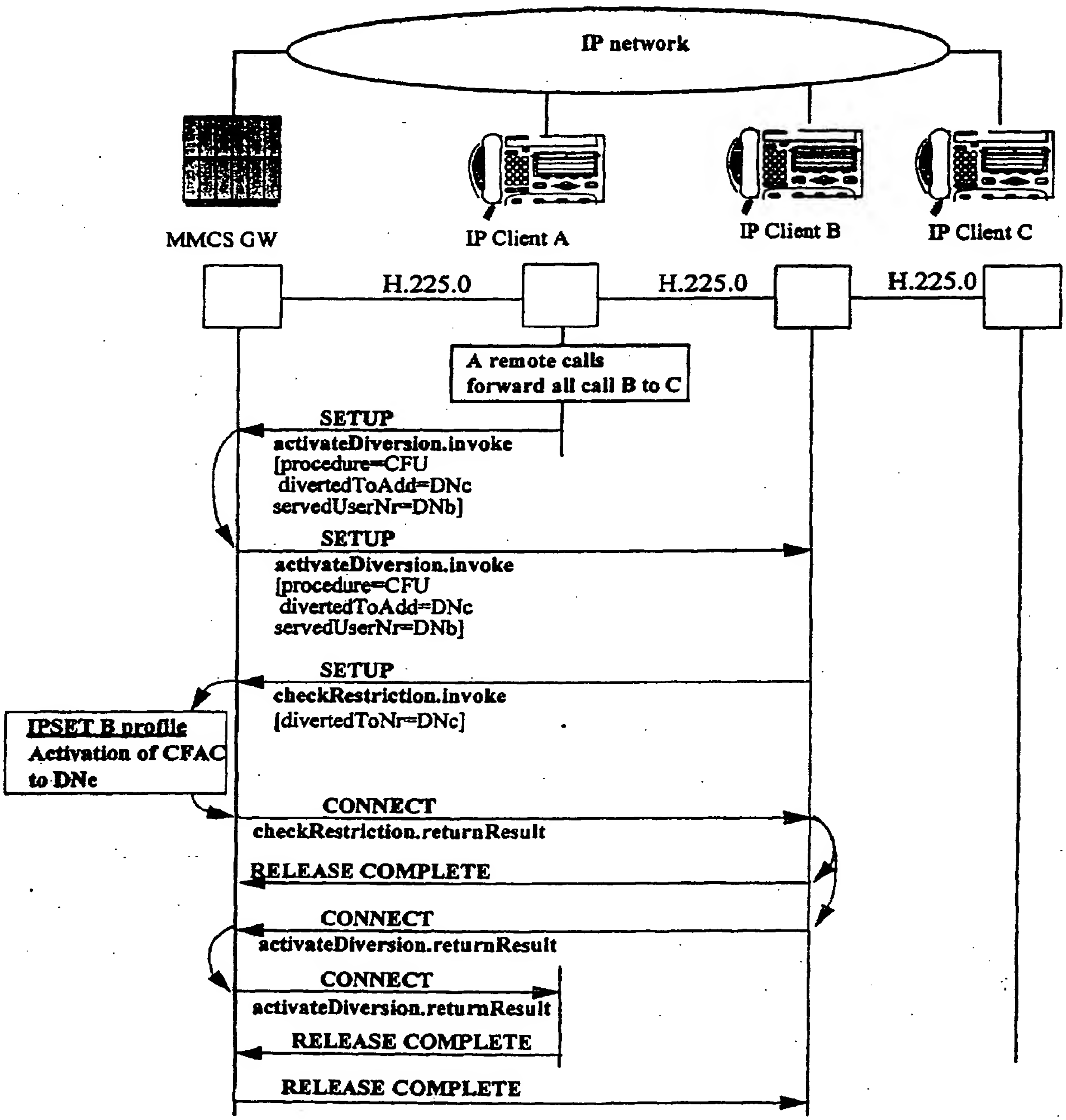

IP network
MMCS GW
IP Client A
IP Client B
H.225.0
H.225.0
A activates call forward all call to B
SETUP
checkRestriction.invoke
[divertedToNr=DNb]
IPSET A profile
Activation of CFAC to DNb
CONNECT
checkRestriction.returnResult
RELEASE COMPLETE

Fig. 42



IP network
MMCS GW
IP Client A
IP Client B
IP Client C
H.225.0
H.225.0
H.225.0
A remote calls forward all call B to C
SETUP
activateDiversion.invoke
[procedure=CFU
divertedToAdd=DNc
servedUserNr=DNb]
SETUP
activateDiversion.invoke
[procedure=CFU
divertedToAdd=DNc
servedUserNr=DNb]
SETUP
checkRestriction.invoke
[divertedToNr=DNc]
IPSET B profile
Activation of CFAC
to DNc
CONNECT
checkRestriction.returnResult
RELEASE COMPLETE
CONNECT
activateDiversion.returnResult
CONNECT
activateDiversion.returnResult
RELEASE COMPLETE
RELEASE COMPLETE

Fig. 43

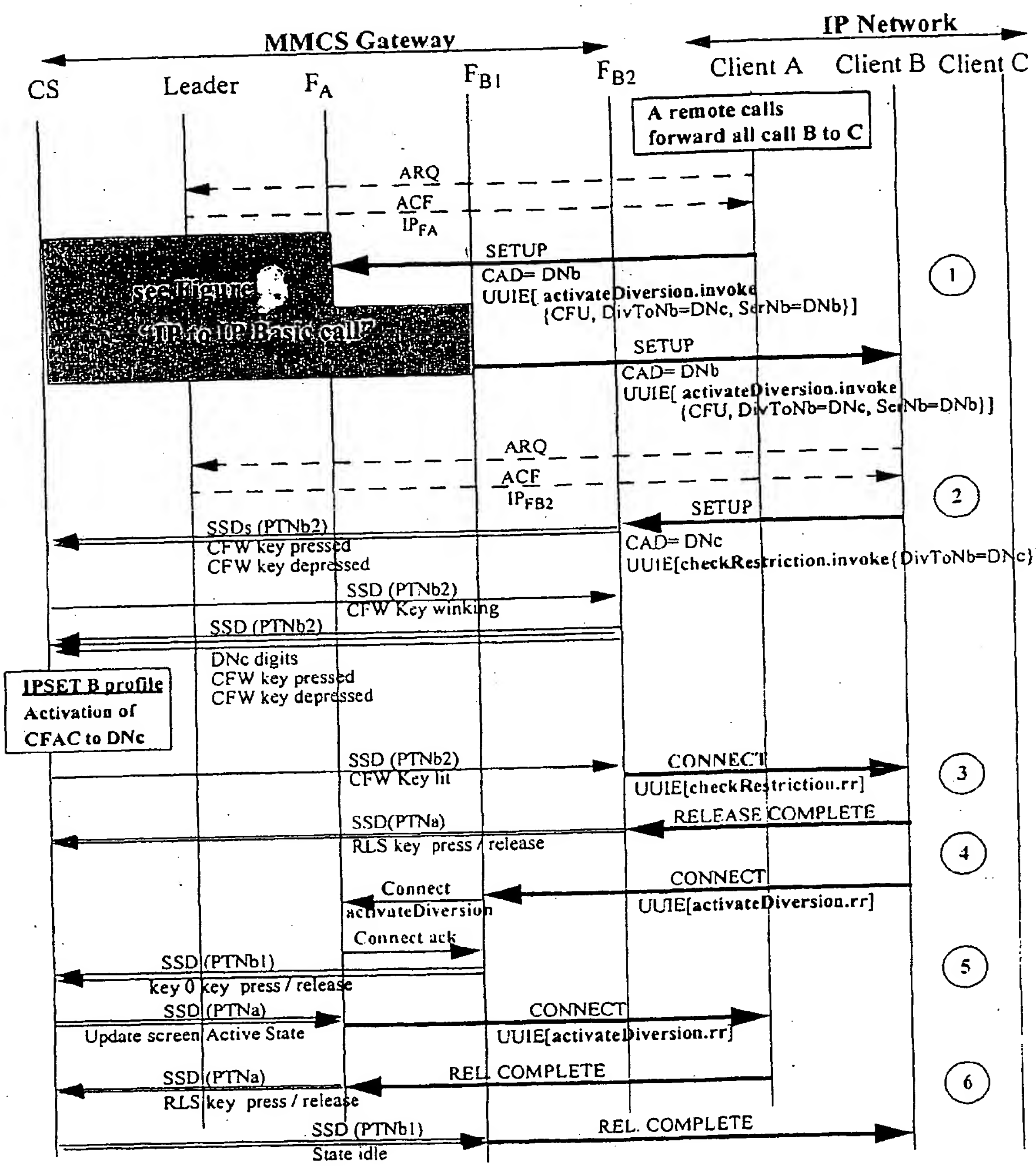

MMCS Gateway
IP Network
CS
Leader
F_A
F_{B1}
F_{B2}
Client A
Client B
Client C
A remote calls forward all call B to C
ARQ
ACF
IP_{FA}
SETUP
CAD= DNb
UUIE[activateDiversion.invoke {CFU, DivToNb=DNc, SerNb=DNb}]
see Figure
SIP to IP Basic call
1
SETUP
CAD= DNb
UUIE[activateDiversion.invoke {CFU, DivToNb=DNc, SerNb=DNb}]
ARQ
ACF
IP_{FB2}
2
SETUP
CAD= DNc
UUIE[checkRestriction.invoke{DivToNb=DNc}]
SSDs (PTNb2)
CFW key pressed
CFW key depressed
SSD (PTNb2)
CFW Key winking
SSD (PTNb2)
DNc digits
CFW key pressed
CFW key depressed
IPSET B profile
Activation of CFAC to DNc
SSD (PTNb2)
CFW Key lit
CONNECT
UUIE[checkRestriction.rr]
3
SSD(PTNa)
RLS key press / release
RELEASE COMPLETE
4
CONNECT
UUIE[activateDiversion.rr]
Connect
activateDiversion
Connect ack
SSD (PTNb1)
key 0 key press / release
5
SSD (PTNa)
Update screen Active State
CONNECT
UUIE[activateDiversion.rr]
SSD (PTNa)
RLS key press / release
REL COMPLETE
6
SSD (PTNb1)
State idle
REL. COMPLETE

Fig. 44